Endpoint Security Policies Reference

ZENworks® 11 Support Pack 2

July 2, 2012

Novell®

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2007-2012 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This *Novell ZENworks 11 SP2 Endpoint Security Policies Reference* provides information to help you create, manage, and publish security policies.

The information in this guide is organized as follows:

Audience

This guide is written for the ZENworks Endpoint Security Management administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

ZENworks Endpoint Security Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the ZENworks 11 documentation Web site (http://www.novell.com/documentation/zenworks11).

Concepts

Novell ZENworks 11 Endpoint Security Management secures and protects Windows workstation devices from security risks regardless of their location. This protection is provided through security policies that you create and assign to workstation devices and users.

The following sections introduce the security policy concepts you need to understand to successfully protect your managed workstation devices.

1 Security Policies vs. Configuration Policies

ZENworks includes three categories of policies: Windows security policies, Windows configuration policies, and Linux configuration policies. The security policies control security-related functionality for Windows workstation devices. The configuration policies control configuration settings for Windows and Linux devices.

ZENworks Endpoint Security Management uses all 11 security policies but only 3 of the configuration policies: Dynamic Local User policy, Windows Group policy, and ZENworks Explorer Configuration policy.

This guide helps you manage the security policies. For information about managing the configuration policies, see the he *ZENworks 11 SP2 Configuration Policies Reference*.

2 Types of Security Policies

There are security policies that control a range of security-related functionality for Windows workstation devices. You can use all or some of the policies, depending on your organization's needs.

Policy	Purpose
Application Control	Blocks execution of applications or denies Internet access to applications. You specify the applications that are blocked or denied Internet access.
Communication Hardware	Disables the following communication hardware: 1394-Firewire, IrDA-Infrared, Bluetooth, serial/parallel, dialup, wired, and wireless. Each communication hardware is configured individually, which means that you can disable some hardware types (for example, Bluetooth and dialup) while leaving others enabled.
Data Encryption	Enables data encryption of files on fixed disks and removable storage devices. With fixed disks, you specify the folders (referred to as *Safe Harbor folders*) that provide encryption; all other fixed disk folders are unaffected.
Firewall	Controls network connectivity by disabling ports, protocols, and network addresses (IP and MAC).
Storage Device Control	Controls access to CD/DVD drives, floppy drives, and removable storage drives. Each storage device type is configured individually, which means that you can disable some and enable others.
USB Connectivity	Controls access to USB devices such as removable storage devices, printers, input devices (keyboards, mice, etc). You can specify individual devices or groups of devices. For example, you can disable access to a specific printer and enable access to all SanDisk USB devices.
VPN Enforcement	Enforces a VPN connection based on the device's location. For example, if the device's location is unknown, you can force a VPN connection through which all Internet traffic is routed.
Wi-Fi	Disables wireless adapters, blocks wireless connections, controls connections to wireless access points, and so forth.

In addition to the above security policies, the following security policies help protect and configure the ZENworks Endpoint Security Agent. The Endpoint Security Agent enforces security policies on a workstation device.

Policy	Purpose
Security Settings	Protects the Endpoint Security Agent from being tampered with and uninstalled.
	This policy is not used with ZENworks 11 SP2 Endpoint Security Agents. The ZENworks 11 SP2 Endpoint Security Agent's security settings are not applied as a policy; instead, they are applied as ZENworks Agent settings (ZENworks Control Center > Configuration > Management Zone Settings > Device Management > ZENworks Agent).
	This policy is retained in ZENworks 11 SP2 to provide support for devices that are still running the ZENworks 11 or ZENworks 11 SP1 Endpoint Security Agent. Those versions of the agent continue to use the Security Settings policy.
Location Assignment	Provides a list of predefined locations for the Endpoint Security Agent. ZENworks Endpoint Security Management lets you associate different security policies with different locations. For example, you might have an Office location and a Remote Office location; you also have a default Unknown location. The Endpoint Security Agent evaluates its current network environment to see if it matches any of the locations included in the Location Assignment policy. If so, the security policies associated with the matched location are applied. If not, the security policies associated with the Unknown location are applied.

3 Locations

The ZENworks 11 Adaptive Agent is location aware. This means that the agent can compare its current network environment against locations you defined. If the network environment matches one of the defined locations, the agent assigns that location to the device. If the network environment does not match a defined location, the agent assigns the Unknown location to the device.

The Endpoint Security Agent inherits the location assignment from the Adaptive Agent. This enables the Endpoint Security Agent to enforce different security policies at different locations. For example, you might choose to enforce different firewall settings for a stationary device located within your corporate office than for a mobile device that moves among less secure, unknown locations.

Most security policies can be designated as either location-based policies or global policies. A location-based policy is applied only if the device's location matches one of the locations identified in the policy. A global policy is applied regardless of the device's location.

Global or Location-based Policies	Global-only Policies
Application Control	Data Encryption
Communication Hardware	Security Settings
Firewall	Location Assignment
Storage Device Control	VPN Enforcement
USB Connectivity	
Wi-Fi	

4 User, Device, and Zone Policy Assignments

You can assign security policies to users, workstation devices, and the Management Zone:

- **User assignment:** A user-assigned policy follows the user. When the user logs in through the ZENworks Adaptive Agent on any device, the user-assigned policies are applied.

- **Device assignment:** A device-assigned policy follows the device. When the Adaptive Agent connects to the Management Zone, the device-assigned policies are applied.

  Security policies apply to workstation devices only. If you assign a security policy to a server device, it is not applied.

- **Zone assignment:** A zone-assigned policy is a default policy. It is evaluated after all user-assigned and device-assigned policies of that type.

Assignments to users and workstation devices are called *direct* assignments. You can also assign security policies to workstation folders and groups. When a user or workstation device is a member of a folder or a group, it inherits the assigned policies. These are called *inherited* assignments.

Assignments to the Management Zone can be made at the Management Zone, on a workstation device folder, and on a workstation device. This enables you to assign different default policies to different devices within your Management Zone.

Simply because a policy is assigned to a workstation device, the device's user, or the Management Zone does not mean that it will be enforced on the device. When multiple policies of the same type are applied to a workstation device through different assignments, the Endpoint Security Agent must determine a single *effective policy* to enforce on the device. Effective policies are discussed in Chapter 5, "Effective Policies," on page 19.

5 Effective Policies

Because of the flexibility in assigning security policies (see Chapter 4, "User, Device, and Zone Policy Assignments," on page 17), it is possible for multiple security policies of the same type to be applied to a device through different sources. For example, one Firewall policy might be assigned to a workstation device, a second Firewall policy to the device's user, and a third Firewall policy to a device group in which the device is a member. Because of multiple assignments, the ZENworks system must determine the *effective* policy for the device. The Endpoint Security Agent can then enforce the one effective policy on the device.

Determination of the effective policy is based on *ordering* and *merging* rules. These are discussed in the following sections:

5.1 Ordering

Policies are applied to a device through device assignments, user assignments, and zone assignments. Through the application of ordering rules, all of the assigned policies are combined into one list in order of precedence, from most important (highest priority) to least important (lowest priority). There are several steps involved in ordering:

5.1.1 Create Ordered Lists for Device-Assigned and User-Assigned Policies

The order of precedence for device-assigned policies and user-assigned policies is determined by where the assignment occurs in the ZENworks management hierarchy, using the following order of precedence:

1. Object
2. Group
3. Folder

A policy assigned to the object (device or user) precedes a policy assigned to the object's group or folder. Likewise, a policy assigned to an object's group precedes a policy assigned to the object's folder.

The order of precedence also takes into account that each level of the hierarchy includes multiple sublevels. For example, if a device resides in a subfolder of the *Workstations* root folder, it might inherit assignments from both folders. Likewise, the device might be a member of multiple groups. The following table expands the levels to show the complete order of precedence:

Level	Order of Precedence	Example	Details
Object	1. First policy listed 2. Second policy listed 3. Third policy listed	1. Policy B 2. Policy A	The order of precedence for policies assigned to an object is determined by the object's *Assigned Policies* list in ZENworks Control Center. A policy at the top of the list has a higher priority than the same-type policies lower in the list. In the example, Policy B precedes Policy A.
Group	1. Object folder a. First group listed i. First policy ii. Second policy b. Second group listed i. First policy ii. Second policy 2. Parent folder a. First group listed i. First policy ii. Second policy b. Second group listed i. First policy ii. Second policy 3. Root folder a. First group listed i. First policy ii. Second policy b. Second group listed i. First policy ii. Second policy	1. Object folder a. Group 4 i. Policy D ii. Policy C b. Group 1 i. Policy F 2. Parent folder a. Group 3 i. Policy G ii. Policy J	The order of precedence for policies assigned to an object's groups is dependent on two factors: 1) the group locations in the folder hierarchy and 2) the policy ordering within the groups. The first factor is the group locations: ◆ For groups within the same folder, the order of precedence follows their order in the folder list, from top to bottom. ◆ For groups within different folders, the order of precedence follows the folders' order of precedence, with the object's folder preceding any of the object's parent folders. In the example, the resulting group order is 4, 1, 3. The second factor is the policy ordering within the group, which is determined by the group's *Assigned Policies* list. A policy at the top of the list has a higher priority than the same-type policies lower in the list. In the example, the resulting policy order is D, C, F, G, J.

Level	Order of Precedence	Example	Details
Folder	1. Object folder a. First policy listed b. Second policy listed 2. Parent folder a. First policy listed b. Second policy listed 3. Root folder a. First policy listed b. Second policy listed	1. Object Folder a. Policy I b. Policy H 2. Parent Folder a. Policy K 3. Root folder a. Policy R b. Policy S	The order of precedence for policies assigned to a folder corresponds to the order in the folder's *Policy Assignments* list. In the example, Policy I has a higher precedence than Policy J. The precedence of an object's folders is determined by the folder hierarchy. The object's folder has precedence over folders located in folders higher in the folder hierarchy.

Using the example in the above table, the order of precedence for the policies assigned to the object (device or user) is:

1. Policy B
2. Policy A
3. Policy D
4. Policy C
5. Policy F
6. Policy G
7. Policy J
8. Policy I
9. Policy H
10. Policy K
11. Policy R
12. Policy S

5.1.2 Create an Ordered List for Zone-Assigned Policies

For policies assigned to the Management Zone, the order of precedence is determined by the position of the policies in the assignment list. The precedence is from the top to the bottom of the list. For example, if Policy A and Policy B are the same type and Policy B is higher in the list, the order of precedence is Policy B, Policy A.

5.1.3 Resolve the Order of the Device-Assigned and User-Assigned Policy Lists

After the ordered lists are created for each type of assignment (device-assigned, user-assigned, and zone-assigned), the three ordered lists for a single policy type look similar to the following example:

User Assignments	Device Assignments	Zone Assignments
1. Policy E	1. Policy H (Device Last)	1. Policy Q
2. Policy A	2. Policy B (User Only)	
3. Policy I	3. Policy R (Device Only)	
	4. Policy D (User Last)	

The goal of ordering is to have one ordered list per location, so the next step is to combine the three lists. By default, the zone-assignments list is always included as the last (lowest priority) list. The order of the user-assignments list and the device-assignments list is determined by the conflict resolution rules configured on the device assignments. There are four conflict resolution rules:

- **User Last:** The user-assigned policies are applied after the device-assigned policies. This means that the user-assigned policies have a higher priority than the device-assigned policies and therefore come first in the order of precedence.
- **Device Last:** The device-assigned policies are applied after the user-assigned policies. This means that the device-assigned policies have a higher priority than the user-assigned policies and therefore come first in the order of precedence.
- **User Only:** The user-assigned policies are applied and the device-assigned policies are ignored. However, if there are no user-assigned policies, the device-assigned policies are applied.
- **Device Only:** The device-assigned policies are applied and the user-assigned policies are ignored.

When there are multiple device assignments, the conflict resolution rule on the highest-priority device assignment is used. In the table above, Policy H is the highest-priority device assignment. Therefore, the Device Last rule is used and the result is the following ordered list:

1. Policy H (Device Assignment)
2. Policy B (Device Assignment)
3. Policy R (Device Assignment)
4. Policy D (Device Assignment)
5. Policy E (User Assignment)
6. Policy A (User Assignment)
7. Policy I (User Assignment)
8. Policy Q (Zone Assignment)

5.1.4 Create Ordered Lists for Each Assigned Location

At this point in the ordering process, the ordered list includes both location-based policies and global policies. Some policies might be applied in one location, others in another location, and some might be applied globally regardless of location.

Because the Endpoint Security Agent applies only the security policies assigned to the device's current security location, it requires separate ordered lists for each available location (as defined in the Location Assignment policy) and for the global "location." This results in lists similar to the following:

Location 1	Location 2	Location 3	Global
1. Policy H	1. Policy B	1. Policy R	1. Policy Q
2. Policy D	2. Policy D	2, Policy E	
3. Policy I	3. Policy A		
	4. Policy I		

Some policies might apply to multiple locations, such as Policy D that is included in the ordered lists for Location 2 and Location 3.

Creating the ordered lists for each location is the last step in the ordering process. With ordering complete, inheritance can be applied.

5.2 Merging

All security policies, except for the Data Encryption and VPN Enforcement policies, support merging of settings from multiple policies to create the effective policy.

After ordering is complete for a policy type, ordered lists exist for each assigned location and for the "global" location. The Endpoint Security Agent then completes the following process to merge policies and generate the final effective policy for each location:

5.2.1 Apply Inheritance to the Location Ordered Lists

Security policies support inheritance, which is the passing of a setting from one policy to another policy of the same type. This allows settings from multiple policies to be merged into the single effective policy. Without inheritance, the effective policy would simply be the highest priority policy in the ordered list.

A policy setting is either single-valued, such as a Firewall policy's Default Behavior field, or is multi-valued, such as a Firewall policy's *Port/Protocol Rules* list. Single-valued settings can have assigned values, or they can inherit values from higher-level policies. Multi-valued settings can have their own values; in addition, they automatically inherit values from higher-level policies.

Consider the following example, where Policy A, B, and C are listed in order of precedence:

	Policy	Setting 1	Setting 2	List 3
1	A	Inherit	Disable	Item 1, Item 2
2	B	Inherit	Inherit	Item 1, Item 4
3	C	Enable	Enable	Item 3, Item 5
	Effective	Enable	Disable	Item 1, Item 2, Item 3, Item 4, Item 5

To determine the effective policy settings, the policies are evaluated from top (highest priority) to bottom (lowest priority). The first non-inherited setting to be found becomes the effective policy setting.

For Setting 1 (a single-valued setting), Policy A inherits from Policy B, which inherits the Enable value from Policy C. Therefore, the effective value for Setting 1 is Enable.

For Setting 2 (a single-valued setting), Policy A is set to Disable, so the remaining policies are ignored. Therefore, the effective value for Setting 2 is Disable.

For List 3 (a multi-valued setting), the values from all three policy lists are used. Values that are exact matches, such as Item 1, are included only one time. Therefore, the effective values for List 3 are Item 1, Item 2, Item 3, Item 4, and Item 5.

Policy setting inheritance can be blocked at any policy. When it is blocked, inheritance stops at that policy. Consider the following example:

	Policy	Inheritance	Setting 1	Setting 2	List 3
1	D	Allowed	Inherit	Disable	Item 1, Item 2
2	E	Blocked	Enable	Disable	Item 1, Item 4
3	F	Allowed	Inherit	Enable	Item 3, Item 5
	Effective		Enable	Disable	Item 1, Item 2, Item 4

Policy E blocks setting inheritance from any lower priority policies.

For Setting 1 (a single-valued setting), Policy D inherits from Policy E, which blocks inheritance from F. Therefore, the effective value for Setting 1 is Enable.

For Setting 2 (a single-valued setting), Policy D is set to Disable, so the remaining policies are ignored. Therefore, the effective value for Setting 2 is Disable.

For List 3 (a multi-valued setting), the values from Policy D and Policy E are used. The values from Policy F are not used because Policy D blocks the inheritance of those values. Therefore, the effective values for List 3 are Item 1, Item 2, and Item 4.

5.2.2 Merge the Location Effective Policies with the Global Effective Policy

At this point, inheritance has been applied to all of the location ordered lists, including the global ordered list. The result is an effective policy for each location and for the global location.

When you assign policies to locations, you have the option of enabling the *Merge policy with assigned global policies* setting. When it is enabled, this setting causes an effective location policy to inherit any "unset" values from the effective global policy. Consider the following example:

Setting	Location 1 Policy	Location 2 Policy	Location 3 Policy	Global Policy
Setting 1	Enable	Disable	Inherit	Disable
Setting 2	Inherit	Disable	Disable	Disable
Setting 3	Enable	Inherit	Enable	Enable

Any location policy setting whose value is Inherit receives the value from the global policy setting.

Setting 1 in the Location 3 policy is set to Inherit. Therefore, it receives the value (Disable) assigned to Setting 1 in the Global policy. The same is true for Setting 2 in the Location 1 policy and Setting 3 in the Location 2 policy.

5.2.3 Merge Location Effective Policies with Default Effective Policy

The Endpoint Security Agent has a default policy of every type. Generally, the setting values for the default policy cause no change to the device.

If, after inheritance has been applied to all of the assigned policies, a setting value in the effective policy is still set to Inherit, the default value is used. The final result is that every setting value is defined for the effective policy.

6 Policy Versioning

A security policy can have multiple versions. Only one version, called the *published* version, is active at any one time.

When you change the published version of a policy, a Sandbox version is created. The published version remains active until you publish the Sandbox version, at which time it becomes active as the new published version. All old versions are retained until you delete them.

For information about publishing different versions of a policy, see Chapter 15, "Publishing Policies," on page 59.

7 Session Support

Please be aware of security policy support for the following types of sessions:

- **Remote Sessions:** The Endpoint Security Agent does not support user-assigned security policies in remote (non-console) sessions. Only device-assigned policies are applied when logging in to a remote session.

- **Fast User Switching Sessions:** The Endpoint Security Agent does not support user-assigned security policies on devices when Fast User switching is used (that is, switching between user accounts without quitting applications and logging out). On devices where Fast User switching is employed, you should use device-assigned and zone-assigned policies only.

II Policy Deployment

The following sections provide information about deploying security policies to devices in your ZENworks Management Zone.

8 Deployment Best Practices

ZENworks management is based on a Manage by Exception model. This model assumes that a significant number of devices or users have the same base requirements; these base requirements become the rule and are applied to all (or most) devices or users, while the differences are handled as individual exceptions. The following sections provide a best practice approach to deploying security policies through the Manage by Exception model.

Practice 1: Define your security locations

The ZENworks Endpoint Security Agent is location aware. This allows it to apply different security policies based on its detected network environment matching defined locations or a default Unknown location.

If you have locations in which you want to enforce different security policies, you should define them before you begin creating policies. This allows you to design policies that best support your locations.

Because locations apply to multiple areas of Novell ZENworks 11, creation of locations is not covered in this *ZENworks Endpoint Security Management Policies Reference*. For location information, see the *ZENworks 11 SP2 Location Awareness Reference*.

Practice 2: Focus on one policy type at a time

There are 10 types of security policies. Each one covers a specific area of device security. Most contain multiple options and concepts that you need to clearly understand. Taken together, the policies can seem overwhelming. You should choose one policy type and focus on how it needs to be deployed in your organization. Then focus on the next one.

The Security Settings policy protects the Endpoint Security Agent. The Location Assignment policy determines which security locations are available to devices or users. Because of the nature of these two policies, we recommend that you address them first.

Practice 3: Decide on the best assignment method

ZENworks supports both device-assigned and user-assigned security policies. You can assign policies to any devices that are registered in your Management Zone. If your ZENworks system is connected to an LDAP user source, you can assign policies to users defined in the source.

As you plan the deployment of a security policy, you should consider whether it is best assigned to devices or to users:

- **Device Assignment:** Device-assigned policies are applied regardless of the user that is logged in. Be aware that security policies apply to workstation devices only. If you assign a security policy to a server device, it is not applied.
- **User Assignment:** User-assigned policies are applied only when the assigned user is logged in. If the user moves from one device to another, the policies move with the user and are applied when the user logs in to the device.

In some cases, you might need to use both types of assignments. For example, you could create a base Firewall policy and assign it to devices. Then, if you have specific users who have different firewall requirements, you could create the appropriate Firewall policy and assign it to the users.

When the same-type policy (such as a Firewall policy) is assigned to both a device and the device's user, you must decide which policy takes precedence. You do this by specifying the conflict resolution rule on the device-assignment. There are four rules:

- **User Last:** Applies the device-assigned policy first and then the user-assigned policy.
- **Device Last:** Applies the user-assigned policy first and then the device-assigned policy.
- **User Only:** Applies the user-assigned policy. If there is no user-assigned policy, the device-assigned policy is applied.
- **Device Only:** Applies the device-assigned policy. Ignores the user-assigned policy.

Practice 4: Utilize the management hierarchy for assignments

The ZENworks management hierarchy contains four levels:

1. Management Zone
2. Folder
3. Group
4. Object

A device or user (the object) is assigned policies directly. A device or user also inherits policies assigned to its zone or to a folder or group in which the device is a member.

Whenever possible, you should assign a policy at a level (or levels) that encompasses the majority of devices or users to whom the policy applies. For example, if all devices in your organization require data encryption, you might assign a Data Encryption policy to the Management Zone and handle policy exceptions with assignments to device groups or individual devices. However, if only a specific group of devices require data encryption, you might decide to organize those devices into a device group and assign a Data Encryption policy to the device group.

Practice 5: Utilize policy settings inheritance

When you create a policy, you provide each policy setting with a value. This is either an absolute value or the *Inherit* value. The *Inherit* value lets the setting value be inherited from the next higher policy in the policy hierarchy.

If, as suggested in Practice 4, you take advantage of the management hierarchy as you make policy assignments, policy settings inheritance becomes an important tool to successfully combine multiple policies into the one effective policy that is enforced on the device.

For example, assume that you create a base Firewall policy. You assign the policy to the Management Zone so that all devices inherit it. In the policy, you set the ACL value to allow 802.1x protocol packets. However, you have one group of devices for which you need to deny 802.1x protocol packets. You create a second Firewall policy, leave all setting values configured to *Inherit* except for the ACL value which you set to deny 802.1x protocol packets, and assign the Firewall policy to the device group. The Firewall policy assigned to the device group is closest to the device (in the policy hierarchy), so it takes precedence. All values are inherited from the zone Firewall policy except for the 802.1x ACL value, which uses the device group Firewall policy.

Multi-valued settings, such as the *Port/Protocol Rules* list in the Firewall policy, do not include an *Inherit* value. Instead, multi-valued settings are combined. In the previous example, the Port/Protocol Rules lists in the two Firewall policies (the zone policy and the device group policy) would be combined into one list in the effective Firewall policy.

In some cases, you might not want a policy to inherit values from a policy higher in the hierarchy. For example, you might not want the device group Firewall policy to inherit the *Port/Protocol Rules* list from the zone Firewall policy. Therefore, you can configure policies to block inheritance of higher-level policies.

Practice 6: Utilize global policies

A global policy is applied in all locations. A location-based policy is applied only in the locations specified in the policy.

If a policy's settings are not dependent on location, use a global policy. Even if some of the policy's settings are dependent on location, consider using a global policy to set the base policy and then creating location-based policies to override the location-dependent settings. When you use global and location-based policies together, the location-based policy settings override the global policy settings.

As you deploy security policies within your zone, we recommend that you create global policies and assign them at the highest level possible, preferably the zone. The global policies should include the policy settings that provide the base security required by the majority of your organization's devices.

Practice 7: Understand how effective policies are determined

The Endpoint Security Agent enforces one policy of each type on a device. This policy is the *effective* policy, which is determined by evaluating and manipulating all assigned policies (of the same type) according to *ordering* and *inheritance* rules.

To successfully deploy the intended policy to a device, you need to fully understand how assigned policies are going to be ordered based on assignment type (device or user), assignment level (zone, folder, group, and object), and policy location type (global or location-based). You also need to know how policy setting inheritance is applied once the order is determined. These concepts are covered in Section 5, "Effective Policies," on page 19.

Practice 8: Test a policy before rolling it out to all users and devices

To ensure that security policies provide the results that you expect, we recommend that you test them on one or more devices before distributing them to all intended users and devices. For instructions, see Chapter 10, "Testing Security Policies," on page 41.

9 Creating Security Policies

The following instructions explain how to create a new security policy by using the Create New Policy Wizard. In addition to using the wizard, you can create policies by:

- Copying an existing security policy. All original system requirements, details, and settings are copied to the new policy. You can then make any desired modifications to the new policy. See Section 16.2, "Copying a Policy," on page 61.
- Creating a Sandbox version of an existing security policy and then publishing it as a new policy. For information, see Section 15.2, "Publishing a Sandbox Version," on page 59.
- Importing a policy from another Management Zone. All original system requirements, details, and settings (if applicable) are imported to the new policy. For information, see Chapter 19, "Importing and Exporting Policies," on page 69.

To create a security policy by using the Create New Policy Wizard:

1 In ZENworks Control Center, click *Policies* to display the Policies page.

2 In the Policies panel, click *New > Policy* to launch the Create New Policy Wizard.

Policies > Create New Policy

Create New Policy
Step 1: Select Platform

Select the platform for which you want to create a policy.

Platform:
Linux
Windows

Description:
Linux - Create a policy for Linux devices.

<< Back   Next >>   Cancel
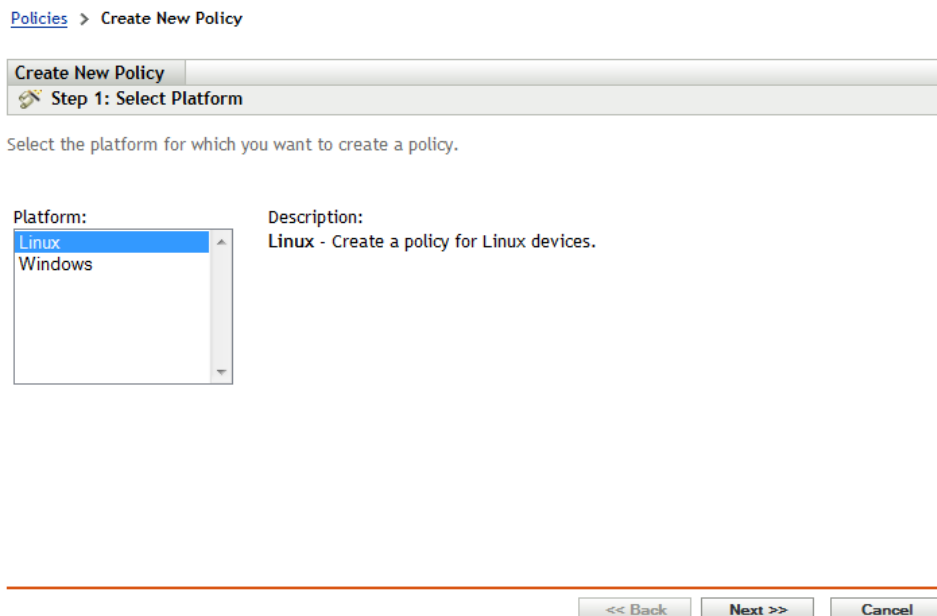
3 On the Select Platform page, select *Windows*, then click *Next*.

4 On the Select Policy Category page, select *Windows Endpoint Security Policies*, then click *Next*.

5 On the Select Policy Type page, select the type of policy you want to create, then click *Next*.

Application Control Policy: Blocks execution of applications or denies Internet access to applications. You specify the applications that are blocked or denied Internet access.

Communication Hardware Policy Disables wireless adapters, blocks wireless connections, controls connections to wireless access points, and so forth.

Data Encryption Policy: Enables data encryption of files on fixed disks and removable storage devices. With fixed disks, you specify the folders (referred to as *Safe Harbor folders*) that provide encryption; all other fixed disk folders are unaffected.

Firewall Policy: Controls network connectivity by disabling ports, protocols, and network addresses (IP and MAC).

Location Assignment Policy: Provides a list of predefined locations for the Endpoint Security Agent. ZENworks Endpoint Security Management lets you associate different security policies with different locations. For example, you might have an Office location and a Remote Office location; you also have a default Unknown location. The Endpoint Security Agent evaluates its current network environment to see if it matches any of the locations included in the Location Assignment policy. If so, the security policies associated with the matched location are applied. If not, the security policies associated with the Unknown location are applied.

Security Settings Policy: Protects the Endpoint Security Agent from being tampered with and uninstalled.

This policy is not used with ZENworks 11 SP2 Endpoint Security Agents. The ZENworks 11 SP2 Endpoint Security Agent's security settings are not applied as a policy; instead, they are applied as ZENworks Agent settings (ZENworks Control Center > Configuration > Management Zone Settings > Device Management > ZENworks Agent).

This policy is retained in ZENworks 11 SP2 to provide support for devices that are still running the ZENworks 11 or ZENworks 11 SP1 Endpoint Security Agent. Those versions of the agent continue to use the Security Settings policy.

Storage Device Control Policy: Controls access to CD/DVD drives, floppy drives, and removable storage drives. Each storage device type is configured individually, which means that you can disable some and enable others.

USB Connectivity Policy: Controls access to USB devices such as removable storage devices, printers, input devices (keyboards, mice, etc). You can specify individual devices or groups of devices. For example, you can disable access to a specific printer and enable access to all SanDisk USB devices.

VPN Enforcement Policy: Enforces a VPN connection based on the device's location. For example, if the device's location is unknown, you can force a VPN connection through which all Internet traffic is routed.

Wi-Fi Policy: Lets you disable wireless adapters, block wireless connections, control connections to wireless access points, and so forth.

6 On the Define Details page, specify a name for the policy, select the folder in which to place the policy, then click *Next*.

The name must be unique among all other policies located in the selected folder. For additional requirements, see Appendix C, "Naming Conventions in ZENworks Control Center," on page 145.

7 (Conditional) If the Configure Inheritance and Location Assignments page is displayed, configure the following settings, then click *Next*.

Inheritance: Leave the *Inherit from policy hierarchy* setting selected if you want to enable this policy to inherit settings from same-type policies that are assigned higher in the policy hierarchy. For example, if you assign this policy to a device and another policy (of the same type) to the device's folder, enabling this option allows this policy to inherit settings from the policy assigned to the device's folder. Deselect the *Inherit from policy hierarchy* setting if you don't want to allow this policy to inherit policy settings.

Location Assignments: Policies can be global or location-based. A global policy is applied regardless of location. A location-based policy is applied only when the device detects that it is within the locations assigned to the policy.

Select whether this is a global or location-based policy. If you select location-based, click *Add*, select the locations to which you want to assign the policy, then click *OK* to add them to the list.

8 Configure the policy-specific settings, then click *Next* until you reach the Summary page.

For information about a policy's settings, you can click *Help > Current Page* in ZENworks Control Center, or you can see Chapter A, "Security Policy Settings," on page 107.

9 On the Summary page, review the information to make sure it is correct. If it is incorrect, click the *Back* button to revisit the appropriate wizard page and make changes. If it is correct, select either of the following options (if desired), then click *Finish*.

- **Create as Sandbox:** Select this option to create the policy as a Sandbox version. The Sandbox version is isolated from users and devices until you publish it. For example, you can assign it to users and devices, but it is applied only after you publish it. You can also use the Sandbox version to test the policy on devices you've designated as test devices. For information, see Chapter 10, "Testing Security Policies," on page 41.

- **Define Additional Properties:** Select this option to display the policy's property pages. These pages let you define system requirements that must be met before the policy can be assigned to a device, assign the policy to users and devices, and add the policy to policy groups.

10 To test the policy before assigning it to users and devices, see Chapter 10, "Testing Security Policies," on page 41

11 To assign the policy to users and devices, see Chapter 11, "Assigning Security Policies," on page 43.

10 Testing Security Policies

To ensure that security policies provide the results that you expect, we recommend that you test them on one or more devices before distributing them to all intended users and devices.

The best way to test a policy on a device is to apply a Sandbox version of the policy to a test device. The following sections explain how to do this:

- Section 10.1, "Designating Test Devices," on page 41
- Section 10.2, "Assigning Policies to Test Devices," on page 41

10.1 Designating Test Devices

You can designate any managed device in your ZENworks Management Zone as a test device. When a policy is assigned to a test device, the Sandbox version of the policy is applied, not the Published version. If no Sandbox version exists, the Published policy is applied.

To designate a managed device as a test device:

1 In ZENworks Control Center, click *Devices*.

2 In the *Devices* list, select the check box next to the target device, then click *Action > Set as Test*.

10.2 Assigning Policies to Test Devices

1 In ZENworks Control Center, click *Policies* to display the Policies page.

2 Click the policy you want to assign to test devices.

3 Make sure the policy you want to test has a Sandbox version. If it does not, create a Sandbox version by editing an item on the Details page (you can change an item and then change it back) and clicking *Apply*.

4 Assign the policy to test devices:

    4a Click the *Relationships* tab.

    4b In the Device Assignments panel, click *Add*, browse for and select the test devices, then click *OK*.

    4c Select *Device Only* as the policy conflict resolution, then click *Next*.

    4d Select *Enforce policies immediately on all assigned devices*, then click *Finish*.

5 Go to a test device and verify that the policy has been applied and is being enforced as expected.

In addition to performing actions on the device that allow you to observe whether or not the policy is being enforced correctly, you can view the effective policies for the device. This is helpful if multiple policies of the same type are assigned to the device; in this case, the policies are merged into one effective policy that is then enforced. For information about viewing a device's effective policies, see Chapter 12, "Viewing Effective Policies," on page 47.

11 Assigning Security Policies

You can assign security policies to users, workstation devices, and the Management Zone. Security policies do not apply to server devices; if you assign a security policy to a server or server folder, the policy is not applied.

When you assign a policy to a user, it is applied when the user is logged in to a ZENworks Server. When you assign a policy to a device, it is applied when the device starts, regardless of whether or not a user is logged in. When you assign a policy to the Management Zone, it becomes a default policy that is only applied after user-assigned and device-assigned policies.

- Section 11.1, "Assigning Policies to Users," on page 43
- Section 11.2, "Assigning Policies to Devices," on page 44
- Section 11.3, "Assigning Policies to the Management Zone," on page 45

11.1 Assigning Policies to Users

You can assign policies and policy groups to users. This section assumes that you have already created any policy groups you want to assign. If not, see Chapter 20, "Managing Policy Groups," on page 71.

The policy assignment can be directly to a user or indirectly to a user through a group or folder in which the user is a member.

1 In ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, select the check box next to policies and policy groups you want to assign.

3 Click *Action > Assign to User*.

4 Browse for and select the user, user groups, and user folders to which you want to assign the group:

    4a Click ⌐ next to a folder to navigate through the folders until you find the user, group, or folder you want to select.

        If you are looking for a specific item, such as a User or a User Group, you can use the *Items of type* list to limit the types of items that are displayed. If you know the name of the item you are looking for, you can use the *Item name* box to search for the item.

    4b Click the underlined link in the *Name* column to select the user, group, or folder and display its name in the *Selected* list box.

    4c Click *OK* to add the selected devices, folders, and groups to the *Users* list.

5 Click *Next* to display the Finish page.

6 Review the information and, if necessary, use the *Back* button to make corrections to the information.

7 If you want the selected policies to be immediately enforced, select the *Enforce policies immediately on all assigned devices*.

This option causes the policy to be immediately distributed to the assigned users' devices and enforced. If you don't select this option, the policy is distributed and enforced the next time the users' device refreshes its policy information from the ZENworks system, either through a manual refresh or a scheduled refresh.

8 Click *Finish*.

The policies or policies groups are assigned to the selected users, user groups, and user folders. You can view the assignments on the Relationships page of the policies or policy groups.

11.2 Assigning Policies to Devices

Security policies apply to workstation devices only. If you assign a security policy to a server device, it is not applied.

1 In ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, select the check box next to the policies and policy groups you want to assign.

3 Click *Action > Assign to Device*.

4 Browse for and select the devices, device groups, and device folders to which you want to assign the group:

    4a Click ☞ next to a folder to navigate through the folders until you find the device, group, or folder you want to select.

        If you are looking for a specific item, such as a Workstation or a Workstation Group, you can use the *Items of type* list to limit the types of items that are displayed. If you know the name of the item you are looking for, you can use the *Item name* box to search for the item.

    4b Click the underlined link in the *Name* column to select the device, group, or folder and display its name in the *Selected* list box.

    4c Click *OK* to add the selected devices, folders, and groups to the *Devices* list.

5 Click *Next* to display the Policy Conflict Resolution page.

This page lets you select how to resolve conflicts if another policy of the same policy type is assigned to one of the selected devices' users. For example, assume that UserA is assigned WirelessPolicy1. You are now assigning WirelessPolicy2 to DeviceA. If UserA logs in to DeviceA, a decision must be made about which policy (WirelessPolicy1 or WirelessPolicy2) to apply.

6 Select one of the following policy conflict resolution methods:

Device Only: Applies the device-associated policy only. If a user-associated policy exists, it is not applied.

User Only: If a user-associated policy exists, applies the user-associated policy. If no user-associated policy exists, applies the device-associated policy.

7 Click *Next* to display the Finish page, review the information and, if necessary, use the *Back* button to make changes to the information.

If you want the policies to be immediately enforced on all the assigned devices, select *Enforce Policies Immediately on all Assigned Devices*.

8 Click *Finish*.

The policies or policies groups are assigned to the selected devices, device groups, and device folders. You can view the assignments on the Relationships page of the policies or policy groups.

11.3 Assigning Policies to the Management Zone

You can assign security policies to the Management Zone. When determining the effective policies to be enforced on a device, the Zone policies are evaluated after all other assigned policies. For more information about how an effective policy is determined, see Section 5, "Effective Policies," on page 19.

Consider the following situations:

- No Firewall policies are assigned to a device or the device's user (either directly or through a group or folder). The Zone Firewall policy becomes the effective policy for the device and is enforced on the device.

- Firewall policies are assigned to a device and the device's user. Both policies are evaluated and manipulated to determine the effective Firewall policy to apply to the device. After the effective policy is determined from the user-assigned and device-assigned policies, the Zone Firewall policy is used to supply any values that 1) are unset in the effective Firewall policy and 2) are additive (such as the multi-valued Port/Protocol Rules tables).

You can assign Zone policies at three levels. This enables you to assign different Zone policies to different devices within your Management Zone.

- **Management Zone:** The policies you assign at the Management Zone become the Zone policies for all devices, unless you assign different Zone policies at the device folder or device level.

- **Device Folder:** The policies you assign at a device folder override the Management Zone (and any parent device folders) and become the Zone policies for all devices contained within the folder structure, unless you assign different Zone policies for a subfolder or an individual device.

   Security policies apply to workstation devices only. If you assign a security policy to a Server device folder, the policy is not applied to any servers located in the folder.

- **Device:** The policies you assign for an individual device override the Management Zone and device folder and become the Zone policies for the device.

   Security policies apply to workstation devices only. If you assign a security policy to a server device, it is not applied.

In ZENworks Control Center:

1 To assign a Zone policy to the Management Zone, click the *Configuration* tab, click *Endpoint Security Management* (in the Management Zone Settings panel), then click *Zone Policy Settings*.

   or

   To assign a Zone policy to a device folder, click the *Devices* tab, locate the folder in the *Devices* list, then click *Details > Settings > Endpoint Security Management > Zone Policy Settings*.

   or

   To assign a Zone policy to a device, click the *Devices* tab, click the device in the *Devices* list, then click *Settings > Endpoint Security Management > Zone Policy Settings*.

2 If you are assigning a Zone policy to a device folder or device, click *Override settings* to activate the panel.

3 In the list, click *Add*, browse for and select the policy you want to add as a default policy, then click *OK* to add it to the list.

4 After you finish adding default policies, click *Apply* to save the settings.

   By default, Management Zone settings are cached on the ZENworks Server and the cache is updated every 10 minutes. Because of this, if a change is made to a zone setting, devices don't receive the changes until the next cache update, which might be as long as 10 minutes.

For ZENworks Endpoint Security Management, the following are stored as zone settings:

- Zone security policies
- Location and network environment settings
- Effective policy report settings
- Data encryption keys

If you change any of these settings and you want to apply them immediately to a device, you must use the zac command line utility on the device to bypass the ZENworks Server cache and retrieve the new settings. To do so, run the following command on the device:

```
zac ref general bypasscache
```

12 Viewing Effective Policies

Because of the flexibility in assigning security policies to users, devices, and the Management Zone, it is possible for multiple security policies of the same type to be applied to a device through different sources. For example, one Firewall policy might be assigned to a device, a second Firewall policy to the device's user, and a third Firewall policy to a device group in which the device is a member. Because of multiple assignments, the ZENworks system must determine the *effective* policy for the device. The Endpoint Security Agent can then enforce the one effective policy on the device. Chapter 5, "Effective Policies," on page 19 explains the process used to determine an effective policy.

There are two ways that you can view a device's effective policies:

 * **ZENworks Control Center report:** If you have ZENworks Reporting Server installed, you can use the Effective Policy report to view a device's effective policies through ZENworks Control Center. For instructions, see Part V, "Policy Reports," on page 87.

 * **ZENworks Endpoint Security Agent:** You can view a device's effective policies through the Agent Status in the Endpoint Security Agent on the device. This requires the Endpoint Security Agent to have an override password assigned through a Security Settings policy.

   For information about using the Endpoint Security Agent to view effective policies, see "Viewing Effective Policies" in the *ZENworks 11 SP2 Endpoint Security Agent Reference*.
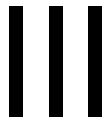
III   Policy Management

The following sections explain how to perform common management tasks for existing security policies. For information about creating security policies, see Part II, "Policy Deployment," on page 31.

13 Editing a Policy's Details

After creating a policy, you can make changes to the policy's details if necessary. Changing a policy's details creates a Sandbox version of the policy. For the changes to be applied, you must publish the Sandbox version.

To edit a policy's details:

1 In ZENworks Control Center, click *Policies* to display the Policies page.

2 In the *Policies* list, click the policy you want to edit.

3 Click the *Details* tab.

4 Make the desired changes.

For information about the policy's details, click the Help button in ZENworks Control Center or see Appendix A, "Security Policy Settings," on page 107.

5 Click *Apply* to save the changes.

6 To publish the changes, click *Publish*, then follow the wizard prompts.

For more information about publishing changes to a policy, see Chapter 15, "Publishing Policies," on page 59.

14 Defining a Policy's System Requirements

You can define requirements, such as operating system, total memory, and processor speed, that a device must meet for the policy to be applied to it. These requirements are in addition to any location-based requirements. For example, consider a policy that is associated with the Office location. When the device is in the Office location, the policy is applied only if it meets the system requirements defined in the policy.

You define requirements through the use of filters. A filter is a condition that must be met by a device in order for the policy to be applied. For example, you can add a filter to specify that the device must have exactly 512 MB of RAM in order for the policy to be applied, and you can add another filter to specify that the hard drive be at least 20 GB in size.

To create system requirements for a policy:

1 In ZENworks Control Center, click the *Policies* tab.

2 Click the policy to display the policy's Summary page.

3 Click the *Requirements* tab.

4 Click *Add Filter*, select a filter condition from the drop-down list, then fill in the fields.

As you construct filters, you need to know the conditions you can use and how to organize the filters to achieve the desired results. For more information, see Section 14.1, "Filter Conditions," on page 53 and Section 14.2, "Filter Logic," on page 57.

5 (Optional) Add additional filters and filter sets.

6 Click *Apply* to save the settings.

Creating or changing system requirements creates a Sandbox version of the policy. For the requirements to be applied, you must publish the Sandbox version.

7 To publish the Sandbox version, click *Publish*, then follow the wizard prompts.

For more information about publishing the Sandbox version of a policy, see Chapter 15, "Publishing Policies," on page 59.

14.1 Filter Conditions

You can choose from any of the following conditions when creating a filter:

- **Architecture:** Determines the architecture of Windows running on the device, either 32-bit or 64-bit. The condition you use to set the requirement includes a property, an operator, and a property value. The possible operators are equals (=) and does not equal (<>). For example, if you set the condition to architecture = 32, the device's Windows operating system must be 32-bit to meet the requirement.

- **Bundle Installed:** Determines if a specific bundle is installed. After specifying the bundle, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the specified bundle must already be installed to meet the requirement. If you select *No*, the bundle must not be installed.

- **Connected:** Determines if the device is connected to a network. The two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the device must be connected to the network to meet the requirement. If you select *No*, it must not be connected.

- **Connection Speed:** Determines the speed of the device's connection to the network. The condition you use to set the requirement includes an operator and a value. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible values are bits per second (*bps*), kilobits per second (*Kbps*), megabits per second (*Mbps*), and gigabits per second (*Gbps*). For example, if you set the condition to `>= 100 Mbps`, the connection speed must be greater than or equal to 100 megabits per second to meet the requirement.

- **Disk Space Free:** Determines the amount of free disk space on the device. The condition you use to set the requirement includes a disk designation, an operator, and a value. The disk designation must be a local drive map (for example, c: or d:). The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible values are bytes (*Bytes*), kilobytes (*KB*), megabytes (*MB*), and gigabytes (*GB*). For example, if you set the condition to `c: >= 80 MB`, the free disk space must be greater than or equal to 80 megabytes to meet the requirement.

- **Disk Space Total:** Determines the amount of total disk space on the device. The condition you use to set the requirement includes a disk designation, an operator, and a value. The disk designation must be a local drive map (for example, c: or d:). The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible values are bytes (*Bytes*), kilobytes (*KB*), megabytes (*MB*), and gigabytes (*GB*). For example, if you set the condition to `c: >= 40 GB`, the total disk space must be greater than or equal to 40 gigabytes to meet the requirement.

- **Disk Space Used:** Determines the amount of used disk space on the device. The condition you use to set the requirement includes a disk designation, an operator, and a value. The disk designation must be a local drive map (for example, c: or d:). The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible values are bytes (*Bytes*), kilobytes (*KB*), megabytes (*MB*), and gigabytes (*GB*). For example, if you set the condition to `c: <= 10 GB`, the used disk space must be less than or equal to 10 gigabytes to meet the requirement.

- **Environment Variable Exists:** Determines if a specific environment variable exists on the device. After specifying the environment variable, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the environment variable must exist on the device to meet the requirement. If you select *No*, it must not exist.

- **Environment Variable Value:** Determines if an environment variable value exists on the device. The condition you use to set the requirement includes the environment variable, an operator, and a variable value. The environment variable can be any operating system supported environment variable. The possible operators are *equal to*, *not equal to*, *contains*, and *does not contain*. The possible variable values are determined by the environment variable. For example, if you set the condition to `Path contains c:\windows\system32`, the Path environment variable must contain the `c:\windows\system32` path to meet the requirement.

- **File Date:** Determines the date of a file. The condition you use to set the requirement includes the filename, an operator, and a date. The filename can be any filename supported by the operating system. The possible operators are *on*, *after*, *on or after*, *before*, and *on or before*. The possible dates are any valid dates. For example, if you set the condition to `app1.msi on or after 6/15/07`, the `app1.msi` file must be dated 6/15/2007 or later to meet the requirement.

- **File Exists:** Determines if a file exists. After specifying the filename, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the specified file must exist to meet the requirement. If you select *No*, the file must not exist.

- **File Size:** Determines the size of a file. The condition you use to set the requirement includes the filename, an operator, and a size. The filename can be any filename supported by the operating system. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible sizes are designated in bytes (*Bytes*), kilobytes (*KB*), megabytes (*MB*), and gigabytes (*GB*). For example, if you set the condition to `doc1.pdf <= 3 MB`, the `doc1.pdf` file must be less than or equal to 3 megabytes to meet the requirement.

- **File Version:** Determines the version of a file. The condition you use to set the requirement includes the filename, an operator, and a version. The filename can be any file name supported by the operating system. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=).

  Be aware that file version numbers contain four components: Major, Minor, Revision, and Build. For example, the file version for `calc.exe` might be 5.1.2600.0. Each component is treated independently. For this reason, the system requirements that you set might not provide your expected results. If you do not specify all four components, wildcards are assumed.

  For example, if you set the condition to `calc.exe <= 5`, you are specifying only the first component of the version number (Major). As a result, versions 5.0.5, 5.1, and 5.1.1.1 also meet the requirement.

  However, because each component is independent, if you set the condition to `calc.exe <= 5.1`, the `calc.exe` file must be less than or equal to version 5.1 to meet the requirement.

- **IP Segment:** Determines the device's IP address. After specifying the IP segment name, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the device's IP address must match the IP segment. If you select *No*, the IP address must not match the IP segment.

- **Logged On To Primary Workstation:** Determines whether the user is logged on to his or her primary workstation. The two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the user must be logged on to his or her primary workstation to meet the requirement. If you select *No*, and no user is logged on to the workstation, the requirement is not met. However, if a user other than the primary user is logged on to the workstation, the requirement is met.

- **Memory:** Determines the amount of memory on the device. The condition you use to set the requirement includes an operator and a memory amount. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The memory amounts are designated in megabytes (*MB*) and gigabytes (*GB*). For example, if you set the condition to `>= 2 GB`, the device must have at least 2 gigabytes of memory to meet the requirement.

- **Novell Client Installed:** Determines if the device is using the Novell Client for its network connection. The two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the device must be using the Novell Client to meet the requirement. If you select *No*, it must not be using the Novell Client.

- **Operating System - Windows:** Determines the architecture, service pack level, type, and version of Windows running on the device. The condition you use to set the requirement includes a property, an operator, and a property value. The possible properties are *architecture*, *service pack*, *type*, and *version*. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The property values vary depending on the property. For example, if you set the condition to `architecture = 32`, the device's Windows operating system must be 32-bit to meet the requirement.

Be aware that operating system version numbers contain four components: Major, Minor, Revision, and Build. For example, the Windows 2000 SP4 release's number might be 5.0.2159.262144. Each component is treated independently. For this reason, the system requirements that you set might not provide your expected results.

For example, if you specify *Operating System - Windows* in the first field, *Version* in the second field, *>* in the third field, and *5.1 -Windows XP Versions* in the last field, you are specifying only the first two components of the version number: Major (Windows) and Minor (5.0). As a result, for the requirement to evaluate to true, the OS must be at least 5.1 (Windows XP). Windows 2003 is version 5.2, so specifying > 5.1 also evaluates to True.

However, because each component is independent, if you specify the version = 5.1, Windows XP SP2 evaluates to False because the actual version number might be 5.1.2159.262144. You can specify the version >= 5.1 to make the requirement evaluate as True because the actual revision component is greater than 0.

When you select the OS version from the drop-down, the Major and Minor components are populated. The Revision and Build components must be typed manually.

- **Primary User Is Logged In:** Determines if the device's primary user is logged in. The two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the primary user must be logged in to meet the requirement. If you select *No*, the user must not be logged in.

- **Processor Family:** Determines the device's processor type. The condition you use to set the requirement includes an operator and a processor family. The possible operators are equals (=) and does not equal (<>). The possible processor families are *Pentium*, *Pentium Pro*, *Pentium II*, *Pentium III*, *Pentium 4*, *Pentium M*, *WinChip*, *Duron*, *BrandID*, *Celeron*, and *Celeron M*. For example, if you set the condition to `<> Celeron`, the device's processor can be any processor family other than Celeron to meet the requirement.

- **Processor Speed:** Determines the device's processor speed. The condition you use to set the requirement includes an operator and a processor speed. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible processor speeds are hertz (*Hz*), kilohertz (*KHz*), megahertz (*MHz*), and gigahertz (*GHz*). For example, if you set the condition to `>= 2 GHz`, the device's speed must be at least 2 gigahertz to meet the requirement.

- **Registry Key Exists:** Determines if a registry key exists. After specifying the key name, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the specified key must exist to meet the requirement. If you select *No*, the key must not exist.

- **Registry Key Value:** Determines if a registry key value exists on the device. The condition you use to set the requirement includes the key name, the value name, an operator, a value type, and a value data. The key and value names must identify the key value you want to check. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible value types are *INT_TYPE* and *STR_TYPE*. The possible value data is determined by the key, value name, and value type.

- **Registry Key and Value Exists:** Determines if a registry key and value exists. After specifying the key name and value, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the specified key and value must exist to meet the requirement. If you select *No*, the key and value must not exist.

- **Service Exists:** Determines if a service exists. After specifying the service name, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the service must exist to meet the requirement. If you select *No*, the service must not exist.

- **Specified Devices:** Determines if the device is one of the specified devices. After specifying the devices, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the device must be included in the specified devices list to meet the requirement (an inclusion list). If you select *No*, the device must not be included in the list (an exclusion list).

14.2 Filter Logic

You can use one or more filters to determine whether the policy should be applied to a device. A device must match the entire filter list (as determined by the logical operators that are explained below) for the policy to be applied to the device.

- Section 14.2.1, "Filters, Filter Sets, and Logical Operators," on page 57
- Section 14.2.2, "Nested Filters and Filter Sets," on page 57

There is no technical limit to the number of filters you can use, but there are practical limits, such as designing a filter structure that is easy to understand and organizing the filters so that you do not create conflicting filters.

14.2.1 Filters, Filter Sets, and Logical Operators

You can add filters individually or in sets. Logical operators, either *AND* or *OR*, are used to combine each filter and filter set. By default, filters are combined using *OR* (as determined by the *Combine Filters Using* field) and filter sets are combined using *AND*. You can change the default and use *AND* to combine filters, in which case filter sets are automatically combined using *OR*. In other words, the logical operator that is to combine individual filters (within in a set) must be the opposite of the operator that is used between filter sets.

You can easily view how these logical operators work. Click both the *Add Filter* and *Add Filter Set* options a few times each to create a few filter sets, then switch between *AND* and *OR* in the *Combine Filters Using* field and observe how the operators change.

As you construct filters and filter sets, you can think in terms of algebraic notation parentheticals, where filters are contained within parentheses, and sets are separated into a series of parenthetical groups. Logical operators (*AND* and *OR*) separate the filters within the parentheses, and the operators are used to separate the parentheticals.

For example, "(u AND v AND w) OR (x AND y AND z)" means "match either uvw or xyz." In the filter list, this looks like:

```
u AND
v AND
w
OR
x AND
y AND
z
```

14.2.2 Nested Filters and Filter Sets

Filters and filter sets cannot be nested. You can only enter them in series, and the first filter or filter set to match the device is used. Therefore, the order in which they are listed does not matter. You are simply looking for a match to cause the policy to be applied to the device.

15 **Publishing Policies**

A policy can include multiple versions:

- **Published version:** The currently active version of the policy. This version is applied to any assigned users and devices.
- **Old versions:** Previously published versions that are not currently active.
- **Sandbox version:** A version that is currently being worked on and has not yet been published as the active version. The Sandbox version is not applied to assigned users and devices until it is published. A Sandbox version can be applied to devices that are designated as test devices. For more information, see Chapter 10, "Testing Security Policies," on page 41.

The following sections explain how to republish an old version and publish a Sandbox version:

- Section 15.1, "Republishing an Old Version," on page 59
- Section 15.2, "Publishing a Sandbox Version," on page 59

15.1 **Republishing an Old Version**

1 In ZENworks Control Center, click *Policies* to display the Policies page.

2 In the *Policies* list, click the policy for which you want to publish a previous version.

3 In the *Displayed Versions* list, select the version you want to publish.

4 Click *Create Sandbox*.

5 (Optional) Make changes to the Sandbox version.

6 Click *Publish*, then follow the wizard prompts.

15.2 **Publishing a Sandbox Version**

When you publish a Sandbox version of a policy, you have the option to publish it as a new version of the current policy or as a completely new policy.

1 In ZENworks Control Center, click *Policies* to display the Policies page.

2 In the *Policies* list, click the policy for which you want to publish a previous version.

3 In the *Displayed Versions* list, select *Sandbox*.

4 Click *Publish* to display the Publish Wizard.

5 If you want to publish the Sandbox version as a new version of the current policy, select *Publish as new version*, then click *Finish*.

or

If you want to publish the Sandbox version as a new policy, select *Publish as new policy*, fill in the new policy information, then click *Next* and follow the prompts to assign the policy to users and devices before clicking *Finish* to create the new policy.

16 Renaming, Copying, and Moving Policies

The following sections provide information to help you rename, copy, and move existing security policies in your ZENworks system:

- Section 16.1, "Renaming a Policy," on page 61
- Section 16.2, "Copying a Policy," on page 61
- Section 16.3, "Moving a Policy," on page 62

16.1 Renaming a Policy

If necessary, you can change a policy's name. Renaming a policy does not affect its assignments. However, it must be republished for the name change to be reflected on devices.

1 In ZENworks Control Center, click the *Policies* tab.

2 Select the check box next to the policy you want to rename, then click *Edit* > *Rename*.

3 In the *Name* field, type the new name.

4 Select the *Publish changed display name immediately* check box to make the change immediately available to devices.

This increments the published policy version and ensures that devices see the name change when the next device refresh occurs. If you do not select this check box, a Sandbox version of the policy is created; the change is not available on devices until after you publish the Sandbox version.

5 Click *OK*.

16.2 Copying a Policy

You can copy a policy to create a new policy. All of the policy's system requirements, details, and settings are copied to the new policy. The relationships (device assignments, user assignments, and policy groups) are not copied.

1 In ZENworks Control Center, click the *Policies* tab.

2 Select the check box next to the policy you want to copy, then click *Edit* > *Copy*.

3 In the *Name* field, type the name for the new policy.

4 Click *OK*.

16.3 Moving a Policy

You can move a policy from one folder in the *Policies* list to another. Moving a policy does not affect the policy's direct assignments to users and devices. It does, however, affect any assignments inherited from its current folder hierarchy.

1 In ZENworks Control Center, click the *Policies* tab.

2 Select the check box next to the policy you want to move, then click *Edit > Move*.

3 Browse for and select the destination folder, then click *OK*.

17 Enabling and Disabling Policies

A security policy can either be enabled or disabled. When a device receives an enabled policy, the Endpoint Security Agent applies the policy. When a device receives a disabled policy, the Endpoint Security Agent ignores the policy.

By default, a security policy is enabled during creation of the policy. The following sections explain how to disable a policy and enable it again.

17.1 Disabling a Policy

When you disable a policy that is currently assigned to users or devices, the policy is ignored after the next device refresh. When you assign a disabled policy to users or devices, it is not applied until you enable it.

1 In ZENworks Control Center, click the *Policies* tab.

2 Select the check box next to the policy that you want to disable.

3 Click *Action > Disable*.

In the *Policies* list, the *Enabled* status for the selected policy is changed to *No*.

17.2 Enabling a Policy

The Endpoint Security Agent does not apply disabled policies that are assigned to the device or the device's user. To have the policy applied, you must enable it:

1 In ZENworks Control Center, click the *Policies* tab.

2 Select the check box next to the policy that you want to enable.

3 Click *Action > Enable*.

In the *Policies* list, the *Enabled* status for the selected policy is changed to *Yes*.

18 Replicating Policies to Content Servers

If you have multiple ZENworks Servers or Satellites functioning as content servers, you can choose to replicate a security policy to all content servers or selected content servers. If a security policy is not replicated to a content server, the policy is not available to any devices that connect to that content server for their policies.

A security policy inherits its content replication settings from its policy folder hierarchy or from the Management Zone. If you do not want it to use the inherited replication settings, you can override the settings on the policy.

The following instructions explain how to override the content replication settings for an individual policy. For information about configuring content replication settings on a policy folder or the Management Zone, see "Content"in the *ZENworks 11 SP2 Primary Server and Satellite Reference*.

To define the replication settings for a security policy:

1 In ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, click the policy to display its properties.

3 Click the *Settings* tab.

Policies > Application Control		
Application Control		
Displayed Version: 0 (Published)		
Summary	Relationships	Requirements	Details	**Settings**

Settings		
Policy Management		
Category	Description	Inherited From
Primary Server Replication	Configure content replication to primary servers.	(System)
Satellite Server Replication	Configure content replication to satellite servers.	(System)
Sandbox Settings	Configure sandbox-specific settings.	N/A

4 Configure the content replication settings for the Primary Servers:

4a In the Policy Management panel, click *Primary Server Replication*.
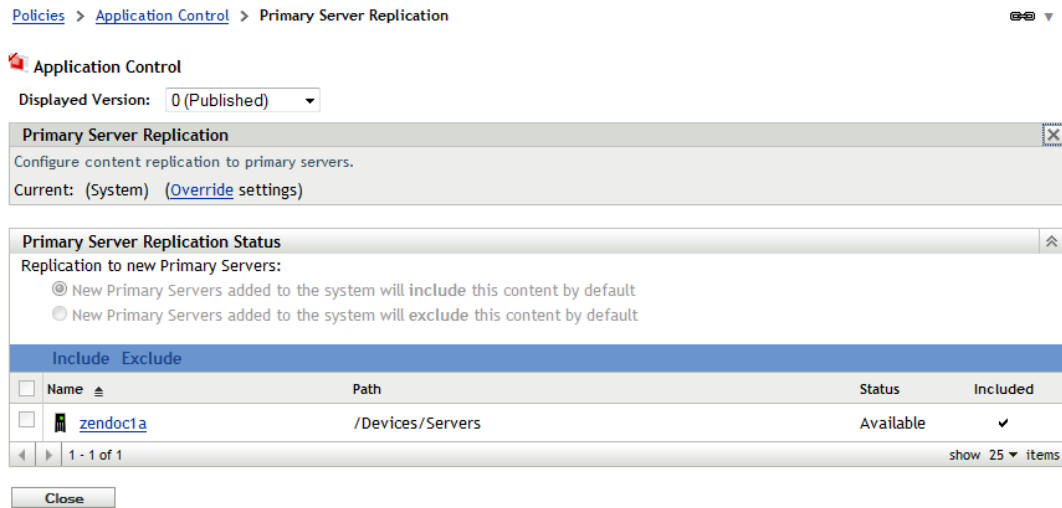
4b Click *Override Settings* to activate the Primary Server Replication Status panel.

4c Select whether or not the policy is replicated to new Primary Servers added to the system.

4d In the list of existing Primary Servers, select the servers that you want to receive the policy, then click *Include*.

A check mark appears in the *Included* column for the selected servers.

4e In the list of existing Primary Servers, select the servers that you don't want to receive the policy, then click *Exclude*.

The *Included* column is left blank to indicate that the servers are not included in the replication of this policy.

4f Click *OK* to save the changes.

5 Configure the content replication settings for Satellites:

5a In the Policy Management panel, click *Satellite Server Replication*.
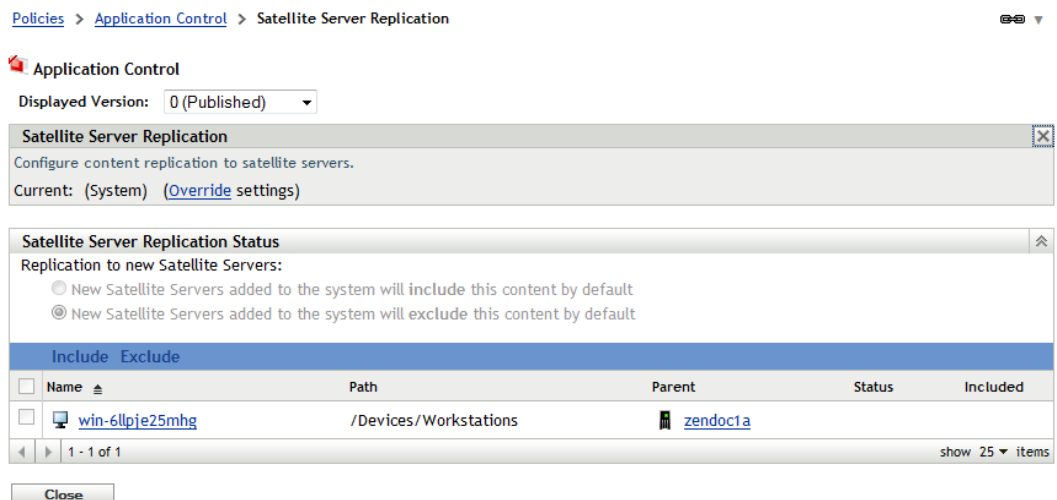
5b Click *Override Settings* to activate the Satellite Server Replication Status panel.

5c Select whether or not the policy is replicated to new Satellite Servers added to the system.

5d In the list of existing Satellite Servers, select the servers that you want to receive the policy, then click *Include*.

A check mark appears in the *Included* column for the selected servers.

5e In the list of existing Satellite Servers, select the servers that you don't want to receive the policy, then click *Exclude*.

The *Included* column is left blank to indicate that the servers are not included in the replication of this policy.

5f Click *OK* to save the changes.

The policy's content replication settings are used only by the ZENworks system and do not affect the actual policy. Therefore, changing the replication settings does not require you to republish the policy to assigned devices and users.

19 Importing and Exporting Policies

You can export security policies from your Management Zone and then import them into another zone or the same zone. This can be useful for exchanging security policies between zones or for backing up important security policies for a single zone.

Exporting and importing is performed through the zman command line utility on the ZENworks Server. The following sections provide instructions:

19.1 Exporting a Policy

When you export a policy, all of the policy data except the relationships (user assignments, device assignments, and policy group membership) is written to an export file. The export file is encrypted so that the data is secure outside of the ZENworks system. Because it is encrypted, you also need to export the policy encryption key with the policy.

Exporting a Policy

1 At a ZENworks Server command prompt, run the following command:

`zman epetf` *(policy path) (XML policy filepath)*

(policy path) - The path (including the filename) of the policy object relative to the Policies root folder. For example, FWpolicy1 or ESMpolicies/DEpolicy4.

(XML policy filepath) - The path (including the filename) where you want to save the XML policy file. If you specify only a filename, the file is saved to the current directory. For example, `firewallpolicy.xml` or `c:\firewallpolicy.xml`.

Examples:

`zman epetf FWPolicy1 c:\FWpolicy1.xml`

`zman epetf ESMpolicies/DEpolicy4 DEpolicy4.xml`

Exporting the Policy Encryption Key

1 At a ZENworks Server command prompt, run the following command:

`zman epektf` *(policy encryption key filepath)*

(policy encryption key file path) - The path (including filename) where you want to save the security policy encryption key file. If you specify only a filename, the file is saved to the current directory. Use any supported filename for the file. The extension is not important; you can use any extension or no extension. For example, `key.txt`, `key.xml`, and `decryption.file` are all valid filenames.

Examples:

```
zman epektf c:\key.txt
zman epektf EncryptionKey.xml
```

19.2   Importing a Policy

When you import a policy from an XML policy file, you can specify the name for the policy and the folder in which to place it.

1 At a ZENworks Server command prompt, run the following command:

```
zman epi (policy name) (policy encryption key filepath) (XML policy file path)
[parent folder]
```

(policy name) - The name to assign to the policy object.

(policy encryption key filepath) - The full path (including the filename) of the security policy encryption key (KMK) file for the Management Zone from which the policy was exported. This file is required to decrypt the encrypted XML file. If the key file is in the current directory, specify only the filename.

(XML policy filepath) - The full path (including the filename) of the encrypted XML policy file. If the file is in the current directory, specify only the filename.

[parent folder] - The Policies folder in which to create the policy object. If you want to create the object in the root folder, ignore this option.

Examples:

```
zman epi FWPolicy c:\key.txt c:\FWpolicy.xml
zman epi DEPolicy key.txt encryptionpolicy.xml esmpolicies/encryption
```

20 Managing Policy Groups

If you have multiple policies that you always want assigned together, you can create a policy group and add the policies as group members. Then, rather than assigning the individual policies, you can assign the policy group.

A policy can be a member of more than one policy group. For example, assume that you have 10 policy groups to accommodate the unique firewall and wireless access needs of various groups within your organization. However, all organizations require the same security for data encryption, so you add the same Data Encryption policy to all of the policy groups.

The following sections provide instructions for managing policy groups:

- Section 20.1, "Creating Policy Groups," on page 71
- Section 20.2, "Adding Policies to Existing Groups," on page 72
- Section 20.3, "Renaming Policy Groups," on page 72
- Section 20.4, "Moving Policy Groups," on page 73
- Section 20.5, "Deleting Policy Groups," on page 73

You assign and remove policy groups for users and devices the same way that you assign and remove policies. For information, see Chapter 11, "Assigning Security Policies," on page 43 and Chapter 22, "Removing Policy Assignments From Users and Devices," on page 79.

20.1 Creating Policy Groups

1. In ZENworks Control Center, click the *Policies* tab.

2. Click *New > Policy Group*.

3. Fill in the fields:

   Group Name: Provide a name for the policy group. The name must be different than the name of any other item (policy, group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.

   For more information, see Appendix C, "Naming Conventions in ZENworks Control Center," on page 145.

   Folder: Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.

   Description: Provide a short description of the policy group's contents. This description displays in ZENworks Control Center.

4. Click *Next* to display the Add Group Members page, then add the policies you want to be members of the group:

   4a. Click *Add* to display the Select Members dialog box.

Because you are adding policies to the group, the Select Members dialog box opens with the `Policies` folder displayed.

4b Click ✐ next to a folder to navigate through the folders until you find the policy you want to select.

If you know the name of the policy you are looking for, you can use the *Item name* box to search for the item. You can add only policies to the group. You cannot add other policy groups to the group.

4c Click the underlined link in the *Name* column to select the policy and display its name in the *Selected* list box.

4d (Optional) Repeat Step 4b and Step 4c to select additional policies.

4e Click *OK* to add the selected policies.

5 Click *Next* to display the Summary page, review the information and, if necessary, use the *Back* button to make changes to the information.

6 (Optional) Select the *Define Additional Properties* option to display the group's properties page after the group is created. You can then configure additional policy group properties, such as assigning the policy group to devices and users.

7 Click *Finish* to create the group.

20.2 Adding Policies to Existing Groups

1 In ZENworks Control Center, click the *Policies* tab.

2 Click the policy group to display its properties.

3 In the Members panel, click *Add* to display the Select Members dialog box.

Because you are adding policies to the group, the Select Members dialog box opens with the `Policies` folder displayed.

4 Click ✐ next to a folder to navigate through the folders until you find the policy you want to select.

If you know the name of the policy you are looking for, you can use the *Item name* box to search for the item. You can add only policies to the group. You cannot add other policy groups to the group.

5 Click the underlined link in the *Name* column to select the policy and display its name in the *Selected* list box.

6 (Optional) Repeat Step 4 and Step 5 to select additional policies.

7 Click *OK* to add the selected policies to the *Members* list.

8 Click *OK* to save the policy group.

20.3 Renaming Policy Groups

You can rename a policy group. Renaming a group does not affect the group's assignments to users and devices.

1 In ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, select the check box next to the policy group you want to rename.

3 Click *Edit*, then click *Rename*.

4 Type the new name in the *Name* field, then click *OK*.

20.4 Moving Policy Groups

You can move a policy group from one folder in the *Policies* list to another. Moving a group does not affect the group's assignments to users and devices.

1 In ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, select the check box next to the policy group you want to move.

3 Click *Edit*, then click *Move*.

4 Select the destination folder for the policy group, then click *OK*.

20.5 Deleting Policy Groups

Deleting a policy group does not delete its policies. It does remove all assignments of the policy group to devices and users.

1 In ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, select the check box next to the policy group.

3 Click *Delete*, then click *OK* to confirm the deletion.

IV Policy Removal

The following sections provide information for removing policy assignments and deleting policies:

21 Removal Best Practices

The following sections provide a best practice approach to removing security policies that have been deployed to devices.

Practice 1: Remove policy assignments before deleting a policy

Deleting a policy automatically removes the policy assignments. However, we recommend that you remove policy assignments before you delete a policy to see if the policy removal has any negative effects on the device. If so, the policy is still available to reassign.

Practice 2: Decrypt files before removing a Data Encryption policy

When you remove a Data Encryption policy from a device, the encryption driver is disabled immediately but the decryption driver remains enabled until the device is rebooted. Users can continue to decrypt files until the device reboots, but no new files can be encrypted. Once the device reboots, encrypted files can no longer be decrypted.

The device is rebooted based on the reboot behavior defined for the ZENworks Adaptive Agent feature installation (ZENworks Control Center > Configuration > Management Zone Settings > Device Management > ZENworks Agent > Reboot Behavior). The one difference is that the forced reboot for a Data Encryption policy occurs after 2 minutes rather than after the 5 minutes stated for agent feature installation.

Before removing a Data Encryption policy from a device, we strongly recommend that you have the device's user decrypt files. This is done by moving the files from Safe Harbor folders and encrypted removable storage devices to non-Safe Harbor (unencrypted) folders on the computer.

If a user fails to decrypt files before the policy is removed and the device reboots, you can use the Administrator version of the File Decryption utility to decrypt the files. For information about the utility, see "File Decryption Utility" in the *ZENworks 11 SP2 Endpoint Security Utilities Reference*.

22 Removing Policy Assignments From Users and Devices

When a policy is assigned to an object (device, user, folder, or group), the assignment is reflected as a *relationship* in the policy's properties and in the object's properties. You can edit the relationships for either the policy or the object to remove the assignment.

The following sections provide instructions for two common assignment removal scenarios:

22.1 Removing Multiple Policy Assignments From the Same Object

The following instructions explain how to remove multiple policy assignments from a single object such as a device, device folder, device group, user, user folder, or user group. For example, these instructions can be used to remove both an Application Control policy assignment and a Firewall policy assignment from a single device.

1 In ZENworks Control Center, click the object (device, device folder, device group, user, user folder, or user group) from which you want to remove policy assignments.

For device and user folders, you need to click *Details* next to the folder name rather than click the name.

2 Click *Relationships*.

3 In the Assigned Policies panel, click the *Direct* tab to ensure that it is active.

The *Direct* tab displays all policies that are assigned directly to the object. Direct assignments are the only assignments you can remove for the object.

4 Select the check box next to the assignments you want to remove, then click *Remove*.

22.2 Removing a Single Policy Assignment From Multiple Objects

The following instructions explain how to remove a single policy assignment from multiple objects such as devices, device folders, device groups, users, user folders, or user groups. For example, these instructions can be used to remove an Application Control policy assignment from a device, a device group, and a user at the same time.

1 In ZENworks Control Center, click the *Policies* tab.

2 In the *Policies* list, click the policy for which you want to remove assignments.

3 Click *Relationships.*

4 In the Device Assignments panel, select the check boxes next to the devices, device groups, and device folders that you no longer want the policy assigned to, then click *Remove.*

5 In the User Assignments panel, select the check boxes next to the users, user groups, and user folders that you no longer want the policy assigned to, then click *Remove.*

23 Removing Policy Assignments From the Management Zone

If you no longer want a policy assigned to the Management Zone, you can remove the policy assignment.

Deleting a policy from the *Policies* list does not remove it from the Zone policy list. When you add a policy to the Zone policy list, a copy of the policy is created for the zone. To remove the assignment from the zone, you must remove the policy from the Zone policy list.

1 If the policy is assigned at the Management Zone, click the *Configuration* tab, click *Endpoint Security Management* (in the Management Zone Settings panel), then click *Zone Policy Settings*.

or

If the Zone policy assignment is on a device folder, click the *Devices* tab, locate the folder in the *Devices* list, then click *Details > Settings > Endpoint Security Management > Zone Policy Settings*.

or

If the Zone policy assignment is on a device, click the *Devices* tab, click the device in the *Devices* list, then click *Settings > Endpoint Security Management > Zone Policy Settings*.

2 In the list, select the policy you want to remove, then click *Remove*.

3 Click *OK* to save your changes.

24 **Deleting Policies**

When you delete a policy, all assignments of the policy to devices and users are removed.

1 In ZENworks Control Center, click the *Policies* tab.

2 Select the check box next to the policy (or policies) that you want to delete.

3 Click *Delete*.

If the policy is assigned as a Zone policy, deleting it from the *Policies* list does not remove it from the Zone policies list. To remove it as a Zone policy, you must also delete it from the Zone policies list. For information, see Chapter 23, "Removing Policy Assignments From the Management Zone," on page 81.

25 Deleting Versions of a Policy

When you make changes to a policy and publish the changes, the policy version is incremented (for example, from version 1 to version 2). The old version is retained in case you want to use it as the basis for a new version of the policy.

If you don't want to keep older versions of a policy, you can delete them. Doing so does not delete the currently published policy and does not affect the policy's assignments.

To delete a version of a policy:

1 In ZENworks Control Center, click the *Policies* tab.
2 Double-click the policy to display its property pages.
3 In the *Displayed Version* field, select the version you want to delete.
4 Click *Delete Selected Version*.

   The selected version is deleted and the published version is displayed.

V Policy Reports

The following sections explain how to configure and generate reports for ZENworks Endpoint Security Management:

26 Configuring Reporting Settings

The reporting settings let you determine which report data the Endpoint Security Agent sends to the ZENworks Server. You can also configure send options such as how often reports are sent, how many are sent at one time, and the locations from which the reports can be sent.

You can configure the reporting settings at three levels:

- **Management Zone:** The reporting settings you define at the Management Zone are used for all devices, unless you override the settings at a device folder or individual device.
- **Device Folder:** The reporting settings you define at a device folder override the Management Zone (and any parent device folders). All devices within the folder use the settings, unless you override the settings on an individual device.
- **Device:** The reporting settings you define for an individual device override the Management Zone and device folder settings.

To configure the reporting settings:

1 Access the appropriate report settings:

- For the Management Zone, click *Configuration* > *Endpoint Security Management* (in the Management Zone Settings panel) > *Endpoint Security Report Settings*.
- For a device folder, click *Devices*, locate the folder in the Devices panel, then click *Details* > *Settings* > *Endpoint Security Management* > *Endpoint Security Reporting Settings*.
- For a device, click *Devices*, click the device in the Devices panel, then click *Settings* > *Endpoint Security Management* > *Endpoint Security Reporting Settings*.

2 If you are configuring the reporting settings for a device folder or a device, click *Override settings* to activate the panel.

3 In the *Endpoint Security Reports* section, select *Effective Policy*.

Currently, the Effective Policy report is the only available report. There are other Endpoint Security reports that you can generate (see Chapter 27, "Generating Reports," on page 91), but those reports do not require collection of information from the Endpoint Security Agent.

A device's Endpoint Security Agent creates an Effective Policy report any time an effective policy for the device changes. For example, if the device's Firewall effective policy changes, a new report is created. Or, if the device's Storage Device Control effective policy changes, a new report is created.

4 In the *Interval for Sending Reports to Server* section, configure at least one of the following settings to enable the Endpoint Security Agent to send reports:

Use Time Interval: Select this option if you want reports sent on a time interval, then specify the interval.

Use Size Interval: Select this option to send reports whenever the combined size of all report files reaches the specified size. The report file size varies based on the number of policy types (Firewall, Data Encryption, and so forth) applied to the device and the amount of data associated with each policy type. Specify the size in kilobytes (for example, 512 KB or 2048 KB). The Endpoint Security Agent evaluates the size of the files every 2 minutes.

You can use one or both intervals. For example, if you set the time interval to 2 days and the size interval to 512 KB, the report files are sent every 2 days. If the files reach 512 KB at some point in the 2-day interval, they are also sent at that point.

5 In the *Throttling for Sending Reports to Server* section, configure the following settings:

Enable Throttling for Sending Reports: Select this option to turn on throttling. Throttling lets you limit the amount of report data that the ZENworks Server accepts from a single device at one time. You can use this to limit server congestion and maintain the performance of your ZENworks Server.

Maximum Number of Reports to Send: Specify the maximum number of reports to send during one session. For example, assume that you set the time interval to 2 days and set this option to 10 reports. Every 2 days, no more than 10 reports are sent regardless of the number of reports that are in the queue. Any remaining reports are saved until the next session two days later.

Interval Before Sending Next Set of Reports: If you want to force all reports to be sent during the current session rather than waiting for the next scheduled session, specify the amount of time to wait before sending the next set of reports. Continuing the example introduced above, if you set this option to 4 hours, the first 10 reports are sent immediately, the second 10 reports are sent 4 hours later, and the final 5 reports are sent four hours after the second set.

If you are using a time interval to initiate when reports are sent, make sure that this setting is less than that time interval.

6 Under *Locations for Sending Reports to Server*, select the *Send reports when the device is in the selected locations* option if you want to limit the locations from which reports can be sent, then click *Add* to add the locations that are allowed.

If you add locations to the list, reports are sent only when the device is in one of the locations and the time or size interval (see Step 4) is met.

7 Under *Delete/Retain Reports*, configure the following settings:

Don't Send if Older Than: Use this option to set an expiration date for unsent reports. Any unsent reports older than the specified age are deleted. This option is useful if you have devices that go long periods of time without connecting to the Management Zone and you don't want to collect old reports from them. Leave the fields blank to send all reports regardless of age.

Delete Reports from Device When Successfully Sent to Server: Select this option to delete reports after they are sent.

Retain Reports on Device for: Select this option to retain reports after they are sent. The reports are moved to an archive folder and retained for the time period you specify. After that time period expires, they are deleted.

8 Click *OK* to save the changes.

27 **Generating Reports**

ZENworks Endpoint Security Management reports are provided by ZENworks Reporting Server. If you have not already installed and configured the Reporting Server, see the *ZENworks 11 Reporting Server Installation Guide*.

The following sections describe the predefined Endpoint Security reports and how to run them. In addition to using predefined reports, you can create custom reports. For information about custom reports, see the *ZENworks 11 System Reporting Reference*.

27.1 Predefined Reports

Report Title	Description
Policy Assignments by Device	Lists all (or selected) devices and their assigned policies. Also lets you view the effective policy settings for a device. For the effective policy settings to be available in the report, you must have enabled effective policy reporting. See Chapter 26, "Configuring Reporting Settings," on page 89.
Policy Assignments by User	Lists all (or selected) users and their assigned policies.
Zone Policy Details	Lists all Zone policies
Effective Policy	Shows a device's effective policy settings for each type of policy.
Application Control Policy Details	Shows the details for one or more Application Control policies.
Communication Hardware Policy Details	Shows the details for one or more Communication Hardware policies.
Data Encryption Policy Details	Shows the details for one or more Date Encryption policies.
Firewall Policy Details	Shows the details for one or more Firewall policies.
Location Assignment Policies Details	Shows the details for one or more Location Assignment policies.
Security Settings Policy Details	Shows the details for one or more Security Settings policies.
Storage Device Policy Details	Shows the details for one or more Storage Device policies.
USB Policy Details	Shows the details for one or more USB Connectivity policies.
VPN Enforcement Policy Details	Shows the details for one or more VPN Enforcement policies.
Wi-Fi Policy Details	Shows the details for one or more Wi-Fi policies.

27.2 Viewing a Predefined Report

The ZENworks Reporting Server must be installed and configured before you can use the predefined reports. For information, see the *ZENworks 11 Reporting Server Installation Guide*.

1 In the ZENworks Control Center, click the *Reports* tab.

2 In the ZENworks Reporting Server panel, click *ZENworks Reporting Server InfoView*.

The InfoView is the main interface for working with the ZENworks Reporting Server reports.

3 Click *Document List*.

4 Navigate to the *All > Public Folders > Novell ZENworks Reports > Predefined Reports > Endpoint Security* folder.

5 Double-click one of the four reports in the folder to generate the report, or open the *Policies* folder and double-click one of the 10 policy-specific reports to generate it.

27.3 Viewing the Effective Policy Report for a Device

The Effective Policy report is accessed through the Policy Assignments by Device report.

1 Generate the Policy Assignments by Device report for the desired device (see Section 27.2, "Viewing a Predefined Report," on page 92).

The report contains a section for each device (if you included multiple devices) that shows the policy assignments for the device. The *Policy Enforced on the Device* column shows the date and time the policy was enforced on the device.

Policy Assignments by Device

Device Name	Primary User	Policy Type	Policy Name	Policy Version	Is Zone policy Assignment?	Effective Date	Policy Enforced on the Device
blr-srm-auto45		ZESM Wireless Policy	WIWI LOC	0 True		Oct 26, 2010 11:47:45 AM	
		ZESM Wireless Policy	WIWI LOC	0 True		Oct 26, 2010 11:48:25 AM	
psamarendra	Shobha	ZESM Comm Hardware Policy	chp LOC	0 False		Oct 26, 2010 10:35:33 AM	2010-10-26 11:05:56.0
	Shobha	ZESM Data Encryption Policy	dep	0 True		Oct 26, 2010 11:47:45 AM	2010-10-26 11:13:53.0
	Shobha	ZESM Data Encryption Policy	dep	0 True		Oct 26, 2010 11:48:25 AM	2010-10-26 11:14:28.0
	Shobha	ZESM Firewall Policy	FP - GLOABL@Version 0	0 False		Oct 26, 2010 10:38:21 AM	2010-10-26 11:40:34.0
	Shobha	ZESM Location Assignment Policy	lap	1 False		Oct 26, 2010 11:47:24 AM	
	Shobha	ZESM Location Assignment Policy	lap	1 True		Oct 26, 2010 11:48:25 AM	
	Shobha	ZESM Location Assignment Policy	lap@Version 0	0 False		Oct 26, 2010 10:39:00 AM	
	Shobha	ZESM Location Assignment Policy	lap@Version 0	0 True		Oct 26, 2010 10:58:43 AM	
	Shobha	ZESM Location Assignment Policy	lap@Version 0	0 True		Oct 26, 2010 11:04:02 AM	
	Shobha	ZESM Location Assignment Policy	lap@Version 0	0 True		Oct 26, 2010 11:47:45 AM	
	Shobha	ZESM Security Settings Policy	ssp	0 False		Oct 26, 2010 10:40:10 AM	
	Shobha	ZESM Security Settings Policy	ssp	0 True		Oct 26, 2010 11:04:02 AM	

Reported by Administrator at 10/27/10 8:24:54 PM GMT+05:30   2/5

2 In the *Policy Enforced on the Device* column, click the most recent date to display the most recent Effective Policy report for the device.

Novell. ZENworks.

ZENworks Endpoint Security Effective Policy

Application Control Policy
Communication Hardware Policy
Firewall Policy
Data Encryption Policy
VPN Policy
Storage Device Control Policy
Location Assignment Policy
Wi-Fi ® Policy
USB Connectivity Policy
Security Settings Policy

Application Control Policy

Location - SDF

Applications

Behavior	Application

Location Source

Type		Name	Identifer	Version	Source
Locaiton Assignment		lap	8f3e7b7a62a15417b65aae6f92af718c	0	Device

Merged Policies

Type		Name	Identifer	Version	Source
Locaiton Assignment		lap	8f3e7b7a62a15417b65aae6f92af718c	0	Device
Application Control		acp - LOC1	b724cd5259169b9a4f8c6daaf0c8fe2e	0	Device

The report includes a section for each policy type. Each section includes the following:

Location list: All policies might not be available in all locations. Therefore, the effective policy can be different from one location to another. This list lets you select the location whose effective policy you want to view. The Data Encryption, Security Settings, VPN Enforcement, and Location Assignment policies are global-only policies; they do not have a location list because the effective policy is the same regardless of location.

Policy settings: The location's effective policy settings are displayed in one or more sections after the location list. These settings are a result of the ordering and merging rules used to determine the effective policy.

Location Source: This section lists 1) the Location Assignment policies that are the source of the currently selected location and 2) the policies that are the source for the effective policy settings.

The icon identifies a global policy. The icon identifies a location-based policy. This section is not displayed for policy types that support only global policies (Data Encryption, Security Settings, VPN Enforcement, and Location Assignment).

Merged Policies: This section lists all of the policies available for the available locations, regardless of the currently selected location (or no location for global-only policies). For example, if there are four available locations included in the Location list, the policies that apply to any of the four locations are shown in the list. This list does not change when you change the location to view the effective policy for that location.

VI Data Encryption Key Management

When a Data Encryption policy is applied to a device, the Endpoint Security Agent uses encryption keys to encrypt and decrypt files. The following sections explain encryption key concepts and provide instructions for managing encryption keys:

28 About Data Encryption Keys

When a Data Encryption policy is applied to a device, the Endpoint Security Agent uses encryption keys to encrypt and decrypt files. The following sections explain concepts that can help you better manage the encryption keys for your Management Zone:

- Section 28.1, "Active Key," on page 97
- Section 28.2, "Multiple Zones," on page 97
- Section 28.3, "Key Security," on page 97

28.1 Active Key

A Management Zone can have one or more encryption keys. At any one time, however, there is only one active key. The active key is used to encrypt new files. The non-active keys are retained in order to decrypt files that were encrypted when the non-active keys were the active keys.

For example, assume that Key1 is the active key. All Endpoint Security Agents use Key1 to encrypt files. You then generate a new key, Key2, which automatically becomes the active key. After Key2 is distributed to devices (during an agent refresh), the Endpoint Security Agent uses it to encrypt new files. The agent uses Key1 to open any files encrypted with that key, then updates the files to the active key (Key2).

28.2 Multiple Zones

Encryption keys are specific to Management Zones. This means that a file encrypted in one zone cannot be opened on a device registered in another zone because the two zones do not automatically share keys.

If you have multiple zones and want to enable devices in all zones to open encrypted files regardless of the zone in which they were encrypted, you can manually share encryption keys by exporting them from one zone and importing them into another. For instructions, see Chapter 30, "Exporting Encryption Keys," on page 101 and Chapter 31, "Importing Encryption Keys," on page 103.

28.3 Key Security

If your organization's policies include a requirement for regularly changing encryption keys, you can generate and activate a new key. After doing so, force an agent refresh to immediately distribute the new key to devices. For instructions, see Chapter 29, "Generating a New Encryption Key," on page 99.

29 Generating a New Encryption Key

You can increase data security by regularly generating a new encryption key. The new key becomes the active encryption key, which means that all newly encrypted files use the key as well as all previously encrypted files that are accessed after the new key is generated.

1 In ZENworks Control Center, click *Endpoint Security*.

2 Under *Common Tasks* (in the left navigation pane) click *Encryption: Generate Keys*.

3 Click *OK* to confirm creation of the new key.

The next time a device refreshes its information from the ZENworks Server, the Endpoint Security Agent begins using the new key.

30 Exporting Encryption Keys

The Endpoint Security Agent uses encryption keys to encrypt and decrypt files. You can export the encryption keys from the Management Zone to a key file to:

- Share the encryption keys with another ZENworks Management Zone. This allows users in the second zone to decrypt files that were encrypted in the first zone.
- Use the encryption keys with the administrator version of the ZENworks File Decryption utility. This allows you to recover encrypted files from devices that no longer have the Endpoint Security Agent installed.
- Back up the encryption keys. We recommend that you follow a regular backup schedule in case problems occur with your ZENworks Servers.

To export the encryption keys:

1 In ZENworks Control Center, click *Endpoint Security*.

2 Under *Common Tasks* (in the left navigation pane) click *Encryption: Export Keys*.

3 Specify a name for the key file.

The file requires a .kbk extension. If you do not add the .kbk extension, it is added automatically.

4 Specify a password for the key file.

Make sure you remember the password. It is required in order to import the keys into another Management Zone or reimport them into the current zone (as a restored backup).

5 Click *OK*.

Depending on how your browser is configured to handle saving files, the file might be automatically saved to your browser's download directory or you might be prompted to save it. Follow any prompts to complete the save process.

31 **Importing Encryption Keys**

The Endpoint Security Agent uses encryption keys to encrypt and decrypt files. You can import encryption keys from a key file to:

- ◆ Use the encryption keys from another ZENworks Management Zone. This allows users to decrypt files that were encrypted in the other zone.
- ◆ Restore a backup of the zone's encryption keys.

To import encryption keys:

1 In ZENworks Control Center, click *Endpoint Security*.

2 Under *Common Tasks* (in the left navigation pane) click *Encryption: Import Keys*.

3 In the *File Name* field, click 🔍 to browse for and select the encryption key file.

4 In the *Password* field, specify the file's password.

This password was assigned when the keys were exported to the file.

5 If you want to change your zone's active key to the active key included in the file, select the *Use the active encryption key from the imported file* option.

A Management Zone can have one or more encryption keys. At any one time, however, there is only one active key. The active key is used to encrypt new files. The non-active keys are retained in order to decrypt files that were encrypted when the non-active keys were the active keys.

6 Click *OK*.

VII Appendixes

A

Security Policy Settings

The following sections provide information about the settings for each security policy:

A.1 Application Control Policy

The following instructions assume that you are on the *Configure Application Control Settings* page in the Create New Application Control Policy Wizard (see Chapter 9, "Creating Security Policies," on page 37) or that you are on the *Details* page for an existing Application Control policy (see Chapter 13, "Editing a Policy's Details," on page 51).

The Application Control policy lets you restrict execution and Internet access for applications. Control extends beyond standard executable files (`.exe`) to include other file types such as `.bat`, `.txt`, `.pdf`, `.mpg`, and so forth.

Configuration is done through *application controls*. An application control identifies one or more applications and assigns a behavior to the applications. The supported behaviors are: 1) block file execution, 2) block Internet access, and 3) no restrictions (allow execution and Internet access). The behavior controls all instances of the listed applications, regardless of location (fixed disk, removable storage device, CD/DVD, or network drive).

For example, assume that `App1.exe`, `App2.exe`, and `App3.exe` are instant message applications that you don't want users to run. You could create an application control called Messaging Applications, assign the three applications to the control, and set the behavior to block execution of the applications.

Or, assume that `App4.exe` and `App5.exe` are media applications that access music and video from the Internet. You don't want bandwidth consumed by these types of activities, so you create an application control called Internet Media Applications, assign the two applications to the control, and set the behavior to block Internet access.

Before applying any policy that blocks file execution or Internet access for an application, you should test the policy on a single workstation to ensure that no adverse or unexpected results occur. For example, blocking critical operating system applications can result in a non-functioning operating system. Or, blocking a Microsoft Office application can result in repeated attempts to reinstall the application, which could affect system operation or performance.

The following table provides instructions for managing the policy's application controls:

Task	Steps	Additional Details
Create a new application control	1. Click *Add* > *Create New*. 2. Fill in the following fields: **Name:** Specify a unique name for the control. The name must be different than any other application control. For information about valid characters, see "Naming Conventions in ZENworks Control Center" on page 145. **Description:** This information is optional. You can provide text that helps identify the purpose, creator, or owner of the control. **Default Behavior:** Select one of the following behaviors: ◆ **No Execution:** Blocks the application from executing. Blocks a non-executable file from opening. ◆ **No Internet Access:** Blocks the application from accessing Internet content. ◆ **No Restrictions:** Removes any restrictions (No Execution or No Internet Access) from the application. This enables you to override any restrictions for the application that might be inherited from another Application Control policy. **Applications:** Specify the applications or files to control. To do so, click *New*, type the name of the application or file, then click *OK* to add it to the list. You must specify the full name of the application or file. Partial names and wildcards are not supported. For example, to specify Notepad, you must enter `notepad.exe`, not just `notepad`. Do not specify a path. The control behavior is applied to all instances of the application regardless of location. **Define Another Application Control:** Select this option to create another application control after you finish this one. 3. Click *OK* to save the control. By default, the application control is enabled. If you do not want it enabled, deselect the *Enabled* box. Disabling the application control leaves it in the policy but excludes it from being enforced when the policy is applied to a device.	The following applications cannot be blocked: ◆ `winlogon.exe` ◆ `svchost.exe` ◆ `taskmgr.exe` ◆ `lsass.exe` ◆ `wmiprvse.exe` ◆ `services.exe` ◆ `explorer.exe` ◆ `smss.exe` ◆ `dllhost.exe` ◆ `csrss.exe`

Task	Steps	Additional Details
Copy an existing application control list from another policy	1. Click *Add > Copy Existing*. 2. Select the Application Control policies whose lists you want to copy. 3. Click *OK*.	All application controls included in the selected policies are copied. If necessary, you can edit the copied controls after they are added to the list.
Import an application control from a policy export file	1. Click *Add > Import*. 2. Click the 🔍 button. 3. Click the *Browse* button to display the *File Upload* dialog box. 4. Select the export file containing the application controls you want to import, then click *Open*. 5. In the Select File dialog box, click *OK*. 6. In the Import File dialog box, click *OK* to import the application controls to the list.	All application controls included in the export file are imported. If necessary, you can edit the imported controls after they are added to the list. For information about exporting controls, see Export an application control.
Edit an application control	1. Click the application control name. 2. Modify the fields as desired. 3. Click *OK*.	
Rename an application control	1. Select the check box next to the application control name, then click *Edit > Rename*. 2. Modify the name as desired. 3. Click *OK*.	
Export an application control	1. Select the check box next to the application control name. You can select multiple controls to export. 2. Click *Edit > Export*. 3. Save the file. The default name given to the file is sharedComponents.xml. You can change the name if desired. Do not change the .xml extension.	
Delete an application control	1. Select the check box next to the application control name, then click *Delete*. 2. Click *OK* to confirm deletion of the control.	

A.2 Communication Hardware Policy

The following instructions assume that you are on the *Configure Communication Hardware Settings* page in the Create New Communication Hardware Policy Wizard (see Chapter 9, "Creating Security Policies," on page 37) or that you are on the *Details* page for an existing Communication Hardware policy (see Chapter 13, "Editing a Policy's Details," on page 51).

The Communication Hardware policy controls access for communication hardware, including being able to completely disable a hardware type (Bluetooth, wired, wireless, and so forth) or limit a hardware type to specific adapters.

- Section A.2.1, "Communication Hardware Settings," on page 111
- Section A.2.2, "Disable Adapter Bridging Control Settings," on page 112

A.2.1 Communication Hardware Settings

This panel lets you control which communication hardware is enabled on a device.

General Settings

The General Settings let you configure the access for the following communication hardware:

- **1394 (FireWire):** Controls the IEEE 1394 bus.
- **IrDA:** Controls the infrared access port.
- **Bluetooth:** Controls Bluetooth access if the device is using the Widcomm Bluetooth Stack software driver to provide the access. Other Bluetooth drivers are not supported.
- **Serial/Parallel:** Controls the serial and parallel communication ports.
- **Dialup:** Controls the dialup adapters (modems).
- **Wired:** Controls the wired network adapters. This setting is available only for location-based policies.
- **Wi-Fi:** Controls the Wi-Fi network adapters.

Choose from the following options to configure the communication hardware access. Not all of the options are available for each hardware type.

- **Enable:** Enables access for the hardware. If you select this option for dialup, wired, or Wi-Fi hardware in a location-based policy, you can use the *Approved Adapters* list to restrict access to specific adapters.
- **Disable:** Disables access for the hardware.
- **Inherit:** Inherits this setting from other Communication Hardware policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Communication Hardware policies assigned to the user's groups, folders, or zone.
- **Disable Modems When Wired:** This option is available only for the Dialup setting in a global policy. It disables dialup access if a wired connection is enabled.
- **Disable Wi-Fi When Wired:** This option is available only for the Wireless setting in a global policy. It disables Wi-Fi access if a wired connection is enabled.

Approved Adapters

The *Approved Adapters* list is displayed only in a location-based policy.

By default, if you allow access for dialup, wired, or wireless hardware, all adapters are allowed. If you want to allow only specific adapters, you can add the adapters to the appropriate Approved Adapters lists (wired, Wi-Fi, or dialup).

When you add an adapter to a list (*Wired*, *Wi-Fi*, or *Dialup*), only the adapters in the approved list are allowed. For example, if you add Adapter1 and Adapter2 to the Approved Wi-Fi Adapters list, those two adapters are the only Wi-fi adapters that are allowed communication access.

The following table provides instructions for managing the approved adapter lists:

Task	Steps
Add an adapter	1. Click the tab (*Approved Wired Adapters*, *Approved Wi-Fi Adapters*, or *Approved Dialup Adapters*) where you want to add the adapter.
	2. Click *Add*.
	3. Fill in the following fields to define the adapter:
	Name: Specify the adapter name. Names are limited to 50 characters and are case sensitive.
	The Name field is a partial match field, meaning that the name only needs to match any part of an adapters name for that adapter to be approved. For example, *Adapter1* not only matches *Adapter1* but also matches *Adapter10* and *Acme Adapter100*. The more complete the name, the more limited the matches.
	MAC Address: This field applies only to Wi-Fi and wired adapters; it does not apply to dialup adapters.
	The MAC address, which is a unique identifier assigned by the manufacturer of the network adapter, is optional. You can use it to more narrowly identify the adapter you want to approve.
	Specify the MAC address by using the following format: xx:xx:xx:xx:xx:xx. For example, 01:C0:23:45:67:89.
	4. Click *OK* to add the adapter to the approved list.
Modify an adapter's settings	1. Click the tab (*Approved Wired Adapters*, *Approved Wi-Fi Adapters*, or *Approved Dialup Adapters*) with the adapter you want to modify.
	2. Click the adapter name.
	3. Modify the settings as desired.
	4. Click *OK* to save the changes.
Remove an adapter	1. Click the tab (*Approved Wired Adapters*, *Approved Wi-Fi Adapters*, or *Approved Dialup Adapters*) with the adapter you want to remove.
	2. Select the check box next to the adapter name, then click *Delete*.
	3. Click *OK* to confirm removal of the adapter.

A.2.2 Disable Adapter Bridging Control Settings

This panel lets you prevent a device's network adapters from being bridged. Bridging, which enables the device to act as a hub for access to multiple network segments, can create a significant breach in your network security.

Adapter Bridging

Select one of the following options:

- **Enable:** Enables adapter bridging.
- **Disable:** Disables adapter bridging.
- **Inherit:** Inherits this setting from other Communication Hardware policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Communication Hardware policies assigned to the user's groups, folders, or zone.

Use Disable Adapter Bridging Message

This setting is available only if adapter bridging is disabled.

Select this option to display a message dialog box when adapter bridging is disabled and a user attempts to create a bridge. Use the *Title of Message Window*, *Body*, and *Message Hyperlink* fields to create the message you want displayed.

A.3 Data Encryption Policy

The following instructions assume that you are on the *Configure Data Encryption Settings* page in the Create New Data Encryption Policy Wizard (see Chapter 9, "Creating Security Policies," on page 37) or that you are on the *Details* page for an existing Data Encryption policy (see Chapter 13, "Editing a Policy's Details," on page 51).

The Data Encryption policy lets you configure the data encryption settings applied to a device. You can enable encryption for one or more locations on the device's fixed disk, enable encryption of removable storage devices (RSDs) attached to the device, and provide additional security through passwords.

As you configure Date Encryption policies and apply them to devices, be aware of the following:

- The policy is a device-only policy. It cannot be assigned to users.
- The policy does not support inheritance. The Data Encryption policy that is assigned closest to the device becomes the effective policy for the device. For example, if a Data Encryption policy is assigned to a device and to a group in which the device is a member, the device-assigned policy becomes the effective policy and the policy assigned to the device group is ignored.
- If you decide to remove a Data Encryption policy from a device, it is strongly recommended that the device's user decrypt files prior to removal of the policy. For more information, see Chapter 21, "Removal Best Practices," on page 77.
- When the policy is applied to or removed from a device, the device must be rebooted to enable or disable the encryption drivers. Data encryption does not occur until after this reboot. To facilitate the reboot, the Endpoint Security Agent applies the reboot behavior defined for the ZENworks Adaptive Agent feature installation (ZENworks Control Center > Configuration > Management Zone Settings > Device Management > ZENworks Agent > Reboot Behavior). The one difference is that the forced reboot for a Data Encryption policy occurs after 2 minutes rather than after the 5 minutes stated for agent feature installation.

Refer to the following sections for policy details:

- Section A.3.1, "Enable Policy Password to Allow Decryption," on page 114
- Section A.3.2, "Enable "Safe Harbor" Encryption for Fixed Disks," on page 115
- Section A.3.3, "Enable Encryption for Removable Storage Devices," on page 115

A.3.1 Enable Policy Password to Allow Decryption

By default, any user who successfully logs in to Windows on a device can access the encrypted files on the device. Select this option to require users to also enter a decryption password when the Endpoint Security Agent starts (typically at Windows startup). This password provides an extra layer of security that applies to encrypted files both in fixed disk locations and on removable storage devices.

After you enable the option, the following settings are available:

- **Administrative Decryption Password:** Click *Change* to specify the decryption password. This password enables users to decrypt files on any device to which the policy is applied. You should use a strong password that meets the following requirements:
    - Seven or more characters
    - At least one of each of the four types of characters:
        - Uppercase letters from A to Z
        - Lowercase letters from a to z
        - Numbers from 0 to 9
        - at least one special character ~ ! @ # $ % ^ & * ( ) + { } [ ] : ; < > ? ,. / - = | \ ″

    For example: y9G@wb?

- **Allow User Defined Secondary Decryption Passwords:** Select this option to allow a user to specify a personal decryption password for the device. This password supplements the administrative password. When prompted for the decryption password, a user can enter his or her personal password or the administrative password.

    For best security practices, we recommend that you enable the secondary decryption password. The administrative decryption password can be used on all devices to which this policy is applied. If you distribute it to users, they can decrypt files on their own device and on any other devices covered by this policy. A user's personal (secondary) decryption password can only be used on his or her device.

    IMPORTANT: If you change a published Data Encryption policy and republish it, the user's secondary decryption password is reset and the user is prompted to define the password again.

- **Require strong password:** Select this option to force users to define a password that meets the following requirements:
    - Seven or more characters
    - At least one of each of the four types of characters:
        - Uppercase letters from A to Z
        - Lowercase letters from a to z
        - Numbers from 0 to 9
        - at least one special character ~ ! @ # $ % ^ & * ( ) + { } [ ] : ; < > ? ,. / - = | \ ″
    For example: qZG@3b!

A.3.2 Enable "Safe Harbor" Encryption for Fixed Disks

Select this option to enable encryption of data on a device's fixed disks. A fixed disk is any hard disk installed on the device. If a hard disk is partitioned, each partition is considered a fixed disk.

The Endpoint Security Agent does not encrypt entire fixed disks. Instead, it encrypts files that are stored in designated folders on the fixed disks. These folders are called Safe Harbor folders, or Safe Harbors.

- **Safe Harbor Locations:** Specify the fixed disk locations (folders) that you want encrypted. The Endpoint Security Agent encrypts all files stored in a Safe Harbor folder. If the folder already exists, the Endpoint Security Agent turns it in to a Safe Harbor folder and encrypts any files that already reside in the folder. If the folder doesn't exist, the agent creates the folder.

  Be aware of the following when designating Safe Harbors:

  - It is strongly recommended that you do not define folders such as My Documents, My Music, My Pictures, and My Videos as Safe Harbor folders. These folders are the default folders for many applications. Making them Safe Harbors could result in the encryption of many files that you don't want encrypted, negatively impacting the overall performance of your applications and computer.

  - The `Windows` and `Program Files` folders (and subfolders) are blocked by the Endpoint Security Agent from being included as Safe Harbors. If you specify them in the policy, they are not added as Safe Harbors on the device.

  - If you specify a folder path that contains an invalid directory, the Safe Harbor folder is not created. For example, `con` is a reserved directory name and is therefore invalid. If you specify `encrypted_files\con\documents`, the Safe Harbor folder is not created.

  To specify a location, click *Add*, specify the location in the *Folder Location* field, then click *OK*. The path is relative to the root of any fixed disk partitions.

  For example, if you specify `Encryption Protected Files` as a Safe Harbor folder, the Endpoint Security Agent creates the folder on each fixed disk (C, D, and so forth) on the device.

- **Allow User Specified Folders:** Select this option to allow users to specify folders that they want to use as Safe Harbor locations. This applies to folders on the local fixed disk only, not removable devices or network drives.

A.3.3 Enable Encryption for Removable Storage Devices

Select this option to enable data encryption on removable storage devices (RSDs). When the policy is applied to a device, the Endpoint Security Agent encrypts all data stored on any removable storage device connected to the device.

Removable storage devices include, but are not limited to, USB thumb drives, flash and PCMCIA memory cards, ZIP drives, floppy drives, external CDR drives, digital cameras, and MP3 players.

A device can access encrypted files on any removable storage devices encrypted by other devices in the same ZENworks Management Zone. This is because all devices within a zone receive all encryption keys for the zone. For example, if Laptop1 and Laptop2 are in the same zone, any files encrypted to a removable storage device on Laptop1 can be accessed on Laptop2.

After you enable encryption for removable storage devices, the following options are available:

- **Enable encryption via user-defined password:** Files are always key-encrypted; key encryption enables them to be read on any managed device within your ZENworks Management Zone. You can select this option to enable password encryption of the files as well. Each user supplies their own password to use for the encryption.

  The advantage to password-encrypted files is that they can be read on non-managed devices (no Endpoint Security Agent installed) by using the ZENworks File Decryption utility and supplying the encryption password. To distribute the ZENworks File Decryption utility, you can have it automatically added to each removable storage device (see Copy standalone decryption tool to removable storage devices below).

- **Folder Name:** If you enabled password encryption of files, specify the folder in which to store the files. Only files stored in this folder are password encrypted. Files stored outside of this folder (on the removable storage device) are not password encrypted (but are still key encrypted).

  The folder is created on the root of the removable storage device. You cannot specify a folder path.

- **Require strong password:** Select this option to force users to define a password that meets the following requirements:

    - Seven or more characters
    - At least one of each of the four types of characters:

        - Uppercase letters from A to Z
        - Lowercase letters from a to z
        - Numbers from 0 to 9
        - at least one special character ~ ! @ # $ % ^ & * ( ) + { } [ ] : ; < > ? ,. / - = | \ "

  For example: y9G@wb?

- **Copy standalone decryption tool to removable storage devices:** The ZENworks File Decryption utility is required to decrypt the password-encrypted files on non-managed devices. Select this option to have the decryption utility copied to removable storage devices so that it is readily available to users.

A.4 Firewall Policy

The following instructions assume that you are on the *Configure Firewall Settings* page in the Create New Firewall Policy Wizard or (see Chapter 9, "Creating Security Policies," on page 37) or that you are on the *Details* page for an existing Firewall policy (see Chapter 13, "Editing a Policy's Details," on page 51).

The Firewall policy lets you determine the firewall settings applied to a device.The firewall settings control a device's network connectivity by allowing or blocking ports, protocols, and network addresses (IP and MAC).

A.4.1 Default Behavior

Specify the default behavior for ports and protocols. The default behavior is applied to all ports and protocols unless it is overridden by a port/protocol rule or an Access Control List.

Select one of the following behaviors:

- **Stateful:** Blocks all unsolicited inbound network traffic. Allows all solicited inbound network traffic and all outbound network traffic.

- **Open:** Allows all inbound and outbound network traffic. Because all network traffic is allowed, a device's identity is visible on all ports.

- **Closed:** Blocks all inbound and outbound network traffic. Because all network identification requests are blocked, a device's identity is concealed on all ports.

  If you select this option, you should enable the ZENworks Server ACL and ARP ACL (see Section A.4.4, "Standard Access Control Lists," on page 119) to ensure that the device can communicate with ZENworks Servers to receive content (policies, bundles, and so forth) and upload report data.

- **Inherit:** Inherits this setting value from other Firewall policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting value is inherited from any Firewall policies assigned to the user's groups, folders, or zone.

A.4.2 Disable Windows Firewall and Register Endpoint Security Management Firewall in Windows Security Center

Select *Yes* to turn off the Windows Firewall and register the Endpoint Security Agent as the firewall provider in the Windows Security Center. This ensures that the Firewall policy's settings and the Windows Firewall settings do not conflict and generate unexpected results.

Select *Inherit* to inherit this setting value from other Firewall policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting value is inherited from any Firewall policies assigned to the user's groups, folders, or zone.

Please be aware of the following when using this option:

- On Windows devices that are members of a domain, the GPO setting *Turn On Security Center (Domain PC's Only)* must be enabled. If the setting is not enabled and you apply a Firewall policy that disables the Windows Firewall, the Endpoint Security Agent is unable to turn off the Windows Firewall; the result is that both the Windows and Endpoint Security firewalls are active.

- This setting disables only the Windows Firewall. If the device has other (third-party) firewalls active, those firewalls are not disabled and could conflict with the Endpoint Security firewall. We recommend that you disable any other firewalls.

A.4.3 Port/Protocol Rules

The port/protocol rules let you override the default behavior assigned to ports and protocols. A rule identifies one or more ports or protocols and the behavior to be applied to the ports and protocols.

For example, assume that you want to block streaming media. You would create a Streaming Media rule and close ports 554, 1755, 7070, and 8000 (the common Microsoft and RealMedia streaming media ports) to TCP communication.

The following table provides instructions for managing the policy's port/protocol rules:

Task	Steps	Additional Details
Create a new rule	1. Click *Add* > *Create New*. 2. Fill in the following fields: **Name:** Specify a unique name for the rule. The name must be different than any other rule. For information about valid characters, see Naming Conventions in ZENworks Control Center. **Description:** This information is optional. You can provide text that helps identify the purpose, membership, creator, or owner of the rule. **Default Behavior:** Select one of the following behaviors: ◆ **Stateful:** All unsolicited inbound network traffic is blocked. All outbound network traffic is allowed. ◆ **Open:** All inbound and outbound network traffic is allowed ◆ **Closed:** All inbound and outbound network traffic is blocked **Port/Protocol Types:** Specify the ports and protocols to add to the rule. To do so, click *New*, select the port type (TCP, UDP, or TCP/UDP) or the protocol type (Ether or IP). For TCP, UDP, and TCP/UDP, specify the starting and ending ports, then click *OK* to add the port to the rule. For Ether and IP, specify the starting and ending ether type or protocol type, then click *OK* to add the protocol to the rule. If you want to define a single port or protocol rather than a range, enter only a starting number. **Define Another Rule:** Select this option to create another port/protocol rule after you finish with this one. 3. Click *OK* to save the rule.	
Copy an existing rule from another policy	1. Click *Add* > *Copy Existing*. 2. Select the Firewall policies whose lists you want to copy. 3. Click *OK*.	All rules included in the other Firewall policies are copied. If necessary, you can edit the copied rules after they are added to the list.
Import a rule from a policy export file	1. Click *Add* > *Import*. 2. Click 🔍 to display the Select File dialog box. 3. Click *Browse*, select the export file, then click *OK*. 4. Click *OK* to add the rules to the list.	All rules included in the export file are imported. If necessary, you can edit the imported rules after they are added to the list. For information about exporting rules, see Export a rule.

Task	Steps	Additional Details
Enable or disable a rule	1. Locate the rule in the list 2. In the *Enabled* column, select the check box to enable the rule. or Deselect the check box to disable the rule.	When you add a rule it is enabled by default. You can disable a rule to save it in the policy but no longer apply it.
Edit a rule	1. Click the rule name. 2. Modify the fields as desired. 3. Click *OK.*	
Rename a rule	1. Select the check box next to the rule name, then click *Edit > Rename.* 2. Modify the name as desired. 3. Click *OK.*	
Export a rule	1. Select the check box next to the rule name. You can select multiple rules to export. 2. Click *Edit > Export.* 3. Save the file. The default name given to the file is sharedComponents.xml. You can change the name if desired. Do not change the .xml extension.	
Delete a rule	1. Select the check box next to the rule name, then click *Delete.* 2. Click *OK* to confirm deletion of the rule.	

A.4.4 Standard Access Control Lists

The standard Access Control Lists (ACLs) represent predefined protocol packet types. For each ACL, select one of the following settings. The ACL setting overrides the default behavior and any port/ protocol rules.

 * **Allow:** Allows the ACL's protocol packets.
 * **Inherit:** Inherits this setting from other Firewall policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Firewall policies assigned to the user's groups, folders, or zone.

The following list provides a brief descriptions of each ACL:

 * **802.1x:** Allows 802.1x packets. To overcome deficiencies in Wired Equivalent Privacy (WEP) keys, Microsoft and other companies are utilizing 802.1x as an alternative authentication method. 802.1x is a port-based network access control that uses the Extensible Authentication Protocol (EAP) or certificates. Currently, most major wireless card vendors and many access point vendors support 802.1x. This setting also allows Light Extensible Authentication Protocol (LEAP) and WiFi Protected Access (WPA) authentication packets.
 * **ARP:** Allows Address Resolution Protocol (ARP) packets. Address resolution refers to the process of finding an address of a computer in a network. The address is resolved by using a protocol in which a piece of information is sent by a client process executing on the local

computer to a server process executing on a remote computer. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address. The address resolution procedure is completed when the client receives a response from the server containing the required address.

- **Ethernet Multicast:** Allows Ethernet Multicast packets. Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news. Multicast packets can be distributed by using either IP or Ethernet addresses.

- **ICMP:** Allows Internet Control Message Protocol (ICMP) packets. ICMP packets are used by routers, intermediary devices, or hosts to communicate updates or error information to other routers, intermediary devices, or hosts. ICMP messages are sent in several situations; for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route.

- **IP Multicast:** Allows IP Multicast packets. Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news. Multicast packets can be distributed by using either IP or Ethernet addresses.

- **IP Subnet Broadcast:** Allows Subnet Broadcast packets. Subnet broadcasts are used to send packets to all hosts of a subnetted, supernetted, or otherwise nonclassful network. All hosts of a nonclassful network listen for and process packets addressed to the subnet broadcast address.

- **Logical Link Layer Control:** Allows LLC-encoded packets.

- **SNAP:** Allows SNAP-encoded packets. Subnetwork Access Protocol (SNAP) is an extension of the Logic Link Control (LLC IEEE 802.2) header and is used for encapsulating IP datagrams and ARP requests and replies on IEEE 802 networks.

- **ZENworks Server:** Allows packets sent to and received from the ZENworks Server.

A.4.5 Access Control Lists

You can create custom Access Control Lists (ACLs) to define specific IP or MAC addresses from which unsolicited traffic should always be blocked or should always be allowed. An ACL setting overrides port rules and the default port behavior.

The following table provides instructions for managing the ACLs:

Task	Steps	Additional Details
Create a new ACL	1. Click *Add* > *Create New*. 2. Fill in the following fields: **Name:** Specify a unique name for the Access Control List. For information about valid characters, see Naming Conventions in ZENworks Control Center. **Description:** Provide optional text that helps identify the purpose, membership, creator, or owner. **ACL Behavior:** Select *Trusted* to specify that membership in this ACL allows access. Select *Non-Trusted* to specify that membership in this ACL denies access. **Configure Optional Ports:** By default, the ACL behavior is applied to all ports. For example, if the ACL behavior is trusted, all ports trust the addresses included in the ACL. If you want the ACL to apply to only specific ports, select this option then specify the ports and the behavior for the ports (*Open*, *Closed*, or *Stateful*). This causes the ACL Behavior setting to be ignored in favor of the individual port behavior settings. **Address Types:** Specify the IP and MAC addresses that are members of the ACL. To do so, click *New*, select the type (*IP Address*, *MAC Address*, or *Macro*), specify the appropriate address or select the desired macro, then click *OK*. The macros are predefined IP address groups. For example, *All DHCP* applies the ACL behavior to a device's current DHCP server IP addresses while Default DHCP applies it to the current Default DHCP server IP address. **Define Another Access Control List:** Select this option to create another Access Control List after you finish with this one. 3. Click *OK* to save the Access Control List. By default, the ACL is enabled. If you do not want it enabled at this time, deselect the *Enabled* box.	Use one of the following formats: ◆ xxx.xxx.xxx.xxx: Standard dotted-decimal notation for a single address. For example, 123.45.167.100. ◆ xxx.xxx.xxx.xxx/n: Standard CIDR (Classless Inter-Domain Routing) notation. For example, 123.45.167.100/24 matches all IP addresses that start with 123.45.167. **IMPORTANT**: To enforce the ACL, an IP address range is expanded to individual IP addresses. A large range can consume significant resources on the device and impact performance. To minimize this impact, define ranges that include only the IP addresses you want to control. Use the following format when specifying a MAC address: xx:xx:xx:xx:xx:xx. For example, 01:23:45:67:89:ab.
Copy an existing ACL from another policy	1. Click *Add* > *Copy Existing*. 2. Select the Firewall policies whose ACL you want to copy. 3. Click *OK*.	All ACLs included in the other Firewall policies are copied. If necessary, you can edit the copied ACLs after they are added to the list.

Task	Steps	Additional Details
Import an ACL from a policy export file	1. Click *Add > Import*. 2. Click 🔍 to display the Select File dialog box. 3. Click *Browse*, select the export file, then click *OK*. 4. Click *OK* to add the ACLs to the list.	All ACLs included in the export file are imported. If necessary, you can edit the imported ACLs after they are added to the list. For information about exporting ACLs, see Export an ACL.
Enable or disable an ACL	1. Locate the ACL in the list 2. In the *Enabled* column, select the check box to enable the ACL. or Deselect the check box to disable the ACL.	When you add an ACL it is enabled by default. You can disable an ACL to save it in the policy but no longer apply it.
Edit an ACL	1. Click the ACL name. 2. Modify the fields as desired. 3. Click *OK*.	
Rename an ACL	1. Select the check box next to the ACL name, then click *Edit > Rename*. 2. Modify the name as desired. 3. Click *OK*.	
Export an ACL	1. Select the check box next to the ACL name. You can select multiple ACLs to export. 2. Click *Edit > Export*. 3. Save the file. The default name given to the file is `sharedComponents.xml`. You can change the name if desired. Do not change the `.xml` extension.	
Delete an ACL	1. Select the check box next to the ACL name, then click *Delete*. 2. Click *OK* to confirm deletion of the ACL.	

A.5 Location Assignment Policy

The following instructions assume that you are on the *Configure Allowed Locations* page in the Create New Location Assignment Policy Wizard (see Chapter 9, "Creating Security Policies," on page 37) or that you are on the *Details* page for an existing Location Assignment policy (see Chapter 13, "Editing a Policy's Details," on page 51).

The Location Assignment policy lets you specify the locations against which the Endpoint Security Agent compares its network environment to determine its location. Only the locations included in the Allowed Locations list are considered.

For example, assume that you have defined four locations (*Configuration* tab > *Locations*). Locations 1 through 3 are common locations you want available to all devices, but Location 4 is required by only a few devices. You include the first three locations in this policy and exclude the fourth location. When applying this policy, the Adaptive Agent evaluates the device's current network environment against the three defined locations to determine the location.

A.5.1 Inherit from Policy Hierarchy

ZENworks utilizes a management hierarchy, or structure, that is ordered as follows:

1. Management Zone
2. Folder/Group
3. Device/User

Policies can be assigned at each level. Assignments flow down, which means that policy assignments made at the Management Zone apply to all devices or users in the zone. Likewise, policy assignments made to a folder or group apply to all members of the folder or group. As a result of hierarchical assignments, it is possible for a device or user to be assigned multiple policies of the same type.

The *Inherit from Policy Hierarchy* option determines whether or not this Security Settings policy can inherit settings from Security Settings policies that are higher in the hierarchy. Consider the following table:

Hierarchy Level	Policy	Inheritance Example 1	Inheritance Example 2	Inheritance Example 3
Zone	LocAssignment_1	Yes	Yes	Yes
User Group 1	LocAssignment_2	Yes	No	Yes
User A	LocAssignment_3	Yes	Yes	No

User A is a member of User Group 1 and the Zone. As such, User A is assigned the LocAssignment_1 and LocAssignment_2 policies as well as the directly assigned LocAssignment_3 policy.

Inheritance Example 1: All three of the policies allow for inheritance. Evaluation of policy settings begins with the lowest policy in the hierarchy. In this case, LocAssignment_3 is the lowest policy (because it is assigned directly to User A) and is evaluated first.

If one of the LocAssignment_3 policy settings is configured as *Inherit*, then the setting is inherited from LocAssignment_2; if the LocAssignment_2 setting is configured as *Inherit*, then the setting is inherited from the next policy in the hierarchy, which is LocAssignment_1.

Multi-value policy settings, such as tables, do not have an *Inherit* setting. With multi-value settings, all values from the assigned policies are combined. In this example, any multi-value settings would combine the values from all three policies.

Inheritance Example 2: LocAssignment_2 does not allow for inheritance from the policy hierarchy. This means that LocAssignment_3 and LocAssignment_2 are used when determining User A's Application Control policy settings. The LocAssignment_1 policy is ignored.

Inheritance Example 3: LocAssignment_3 does not allow for inheritance from the policy hierarchy. This means that only LocAssignment_3 is used. The two higher policies (LocAssignment_2 and LocAssignment_3) are not used.

A.5.2 Allowed Locations

You use the *Allowed Locations* list to add the locations that are allowed by this policy. By default, the Unknown location is automatically added to the policy. This enables the device to fail over to the Unknown location if the current network environment does not match any of the policy's locations.

The following table provides instructions for managing the allowed locations:

Task	Steps
Add a location	1. Click *Add* to display the Select Locations dialog box.
	2. Click the locations you want to add to the list.
	You can add only existing locations. Locations are created on the Locations page (*Configuration* tab > *Locations*)
	3. Click *OK* to add the locations.
Modify a location's settings	1. Select the check box next to the location > click *Edit*.
	2. Modify the settings as desired:
	Allow Manual Change: Select *Yes* to let the user change to the location and change from the location. For example, assume the policy includes three locations. This setting is enabled for Location1 and Location2, but not for Location3. If the agent determines the current location to be Location1, the user can manually change to Location2 but not to Location3. This is because Location1 and Location2 both allow manual changes, but Location3 does not. If the agent determines that the location is Location3, the user cannot change the location.
	Select *Inherit* to inherit this setting value from other Location Assignment policies assigned higher in the policy hierarchy.
	Show Location in Agent List: Select *Yes* to include the location in the list of locations displayed when the user right-clicks the agent's Z-icon.
	Select *Inherit* to inherit this setting value from other Location Assignment policies assigned higher in the policy hierarchy.
	Use Location Message: Display a custom message when the agent switches to this location. This message can provide instructions for the user, give details about policy restrictions under this location, or include a hyperlink to more information.
	3. Click *OK*.
Remove a location	1. Select the check box next to the location name, then click *Remove*.
	2. Click *OK* to confirm removal of the location.

A.6 Scripting Policy

The following instructions assume that you are on the *Configure Security Settings* page in the Create New Security Settings Policy Wizard (see Chapter 9, "Creating Security Policies," on page 37) or that you are on the *Details* page for an existing Security Settings policy (see Chapter 13, "Editing a Policy's Details," on page 51).

The Scripting policy lets you run a script (JScript or VBScript) on a device. You can specify the triggers that cause the script to run. Triggers can be based on Endpoint Security Agent actions, location changes, or time intervals.

- Section A.6.1, "Script Settings," on page 125
- Section A.6.2, "Trigger Settings," on page 126

A.6.1 Script Settings

The Script Settings panel lets you define the language, content, and execution space for the script.

Run As

Select whether you want the script to run in the system context or the user context:

- **System:** The script runs with the same rights as a Windows service.
- **User:** The script runs with the rights provided by the current user session.

Language

Select *JScript* or *VBScript* as the scripting language.

Script Content

Click *Edit* to add the script content.

ZENworks supports standard JScript and VBScript coding methods, with the following exceptions.

1. WScript.Echo is not supported because return values can't be sent back to a parent window that is unavailable. Use the Action.Message ZENworks Endpoint Security Management API instead.

2. Access to Shell Objects. Use the following modified nomenclature/call:

```
[JScript]
   Use:
   var WshShell = new ActiveXObject("WScript.Shell");
   Instead of:
   var WshShell = WScript.CreateObject ("WScript.Shell");

[VBScript]
   Use:
   Dim WshShell
   Set WshShell = CreateObject("WScript.Shell")
   Instead of:
   Dim WshShell
   Set WshShell = WScript.CreateObject("WScript.Shell")
```

ZENworks also provides a scripting interface that lets you create advanced scripts. Using the scripting interface, you can determine current state of the Endpoint Security Agent, run actions that change the behavior of the agent or interact with the user, and store variables for use by the script during the current session or across sessions.

For more details about the scripting interface, see the *ZENworks 11 SP2 Endpoint Security Scripting Reference*.

A.6.2 Trigger Settings

The Trigger Settings panel lets you determine when the script runs. There are three types of triggers that initiate execution of the script:

- **Agent Triggers:** Executes the script based on one or more Endpoint Security Agent actions, such as the enforcement of the Scripting policy or the change from one network environment to another.
- **Location Trigger:** Executes the script when changing from one location to another.
- **Time Trigger:** Executes the script according to a specified time interval.

You can use one or more of the trigger types to ensure that the script runs at the appropriate times.

Agent Triggers

The Agent Triggers settings executes the script based on one or more Endpoint Security Agent actions, such as the enforcement of the Scripting policy or the change from one network environment to another. Select one or more of the following actions:

- **Enforcement of this policy:** Executes the script any time this policy is enforced. Enforcement occurs on device startup (zone-assigned and device-assigned policies), user-login (user-assigned policies), and policy updates.
- **Any security policy change:** Executes the script any time the agent receives a change to any of the security policies (Firewall, Communication Hardware, and so forth).
- **Network change:** Executes the script any time the agent detects a network change that could affect the location assignment. This involves changes to the device's actual network environment (IP addresses, access points, and so forth) and the network environment definitions used to determine location.
- **Network connect:** Executes the script any time a network connection occurs. This could be a wired network that is detected after plugging in a network cable, a wireless network detected through an access point, a network detected through a modem, or more.
- **Network disconnect:** Executes the script any time a network disconnection occurs.

Location Trigger

The Location Trigger setting executes the script based on a location change. The trigger consists of two conditions that are evaluated to determine if the script should run:

- The location from which the device is switching. This is referred to as the "from" location.
- The location to which the device is switching. This is referred to as the "to" location.

The script is run only if both the "from" location and "to" location conditions are true.

Enable Location Trigger

Select this option to enable the location trigger.

Run When Switching From

This setting lets you define the first of the two conditions, the "from" locations:

- **Any location:** Select this option if you want all locations to qualify as valid "from" locations.
- **Selected locations:** Select this option if you want to designate one or more specific locations as valid "from" locations.

And When Switching To

This setting lets you define the second of the two conditions, the "to" locations:

- **Any location:** Select this option if you want all locations to qualify as valid "to" locations.
- **Selected locations:** Select this option if you want to designate one or more specific locations as valid "to" locations.

Must Be a Manual Change

A location change can be automatic or manual. An automatic location change occurs when the Endpoint Security Agent detects a change in the network environment that results in a new location assignment. A manual change occurs when a device's user manually selects a new location from the agent's Locations list.

Select this option if you only want the script to run when the user manually changes the location. Any automatic changes will not trigger execution of the script.

Time Trigger

The Time Trigger setting executes the script at a designated interval. The interval begins upon initial enforcement of the policy. If the policy is changed and republished, the interval is restarted.

The interval includes a one-minute boundary, meaning that the script is run within a minute (plus or minus) of the end of the interval.

Select the option to enable it, then enter the interval between each running of the script.

A.7 Security Settings Policy

This policy is not used with ZENworks 11 SP2 Endpoint Security Agents. The ZENworks 11 SP2 Endpoint Security Agent's security settings are not applied as a policy; instead, they are applied as ZENworks Agent settings (ZENworks Control Center > Configuration > Management Zone Settings > Device Management > ZENworks Agent).

This policy is retained in ZENworks 11 SP2 to provide support for devices that are still running the ZENworks 11 or ZENworks 11 SP1 Endpoint Security Agent. Those versions of the agent continue to use the Security Settings policy.

The following instructions assume that you are on the *Configure Security Settings* page in the Create New Security Settings Policy Wizard (see Chapter 9, "Creating Security Policies," on page 37) or that you are on the *Details* page for an existing Security Settings policy (see Chapter 13, "Editing a Policy's Details," on page 51).

The ZENworks Endpoint Security Agent (referred to as the Endpoint Security Agent) is the ZENworks Adaptive Agent module that manages and enforces security policies on a device. This panel lets you configure the security settings for the Endpoint Security Agent.

- Section A.7.1, "Enable Client Self Defense for Endpoint Security Agent," on page 128
- Section A.7.2, "Enable Uninstall Password for Endpoint Security Agent," on page 128
- Section A.7.3, "Enable Password Override for Endpoint Security Agent," on page 129

A.7.1 Enable Client Self Defense for Endpoint Security Agent

Client Self Defense protects the Endpoint Security Agent from being shut down, disabled, or tampered with in any way. If a user performs any of the following activities, the device is automatically rebooted to restore the correct system configuration:

- Using Windows Task Manager to terminate any Endpoint Security Agent processes.
- Stopping or pausing any Endpoint Security Agent services.
- Removing critical files and registry entries. If a change is made to any registry keys or values associated with the Endpoint Security Agent, the registry keys or values are immediately reset.
- Disabling NDIS filter driver binding to adapters.

Select one of the following options:

- **Yes:** Enables Client Self Defense.
- **No:** Disables Client Self Defense.
- **Inherit:** Inherits this setting value from other Security Setting policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting value is inherited from any Security Setting policies assigned to the user's groups, folders, or zone.

A.7.2 Enable Uninstall Password for Endpoint Security Agent

Client Self Defense does not prevent the Endpoint Security Agent from being uninstalled by the agent installation program. If you want to prevent users from removing the Endpoint Security Agent without permission, you must enable an uninstall password.

The uninstall password applies only when a user tries to uninstall the agent at the device. If you use the ZENworks Adaptive Agent features (*Configuration* tab > *Management Zone Settings* > *Device Management* > *ZENworks Agent*) to uninstall the Endpoint Security Agent, the uninstall password is not used.

Select one of the following options:

- **Yes:** Enables an uninstall password. To specify the password, click *Change*, specify and confirm the password, then click *OK* to save it.
- **No:** Disables an uninstall password.
- **Inherit:** Inherits this setting value from other Security Setting policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting value is inherited from any Security Setting policies assigned to the user's groups, folders, or zone.

A.7.3 Enable Password Override for Endpoint Security Agent

Password Override lets you specify a password that overrides the device's currently applied security policies. All policies revert to the Endpoint Security Agent's default policies.

You should not distribute the password to users. Instead, you should use the Override Password Key Generator utility to generate a temporary password key (based on the override password) for a user who needs to override security policies. The password key functions the same as the override password with the added benefit that you can specify when the key expires.

Select one of the following options:

 - **Yes:** Enables an override password. To specify the password, click *Change*, enter and confirm the password, then click *OK* to save it.
 - **No:** Disables the override password.
 - **Inherit:** Inherits this setting value from other Security Setting policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting value is inherited from any Security Setting policies assigned to the user's groups, folders, or zone.

A.8 Storage Device Control Policy

The following instructions assume that you are on the *Configure Storage Device Control Settings* page in the Create New Storage Device Control Policy Wizard (see Chapter 9, "Creating Security Policies," on page 37) or that you are on the *Details* page for an existing Storage Device Control policy (see Chapter 13, "Editing a Policy's Details," on page 51).

This Storage Device Control policy lets you control access to CD/DVD drives, floppy drives, and removable storage drives. For each drive, you can allow full access, allow read access only, disable all access, or default to the global Storage Device Control policy setting.

A.8.1 AutoPlay/AutoRun

The AutoPlay/AutoRun setting can only be configured on a global Storage Device Control policy. It is not available on location-based policies. This means that it is always applied regardless of the device's location.

This setting controls the Windows AutoPlay feature. AutoPlay performs two processes. First, it launches the AutoRun process, which looks for an `autorun.inf` in the root directory and executes the instructions in the file. Second, it looks for specific content (music, video, and pictures) and launches the appropriate application to display or play the content. Select one of the following options:

 - **Enable:** Enables both AutoPlay and AutoRun.
 - **Disable Auto Play:** Disables the AutoPlay feature, including AutoRun.
 - **Disable Auto Run:** Disables the AutoRun feature so that `autorun.inf` instructions are not executed. Launching applications for music, video, and pictures is not disabled.

◆ **Inherit:** Inherits this setting from other Storage Device Control policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Storage Device Control policies assigned to the user's groups, folders, or zone.

A.8.2 Storage Device Categories

You can control access to the following categories of storage devices:

◆ **CD/DVD:** Controls access to any devices listed under *DVD/CD-ROM drives* in Windows Device Manager.

◆ **Floppy Drive:** Controls access to any devices listed under *Floppy drives* in Windows Device Manager.

◆ **Removable Storage:** Controls access to any devices reporting as removable storage under *Disk drives* in Windows Device Manager.

For each storage device, select one of the following options:

◆ **Enable:** Enables read and write access.

◆ **Disable:** Prevents read and write access. When users attempt to access files on the device, they receive an error message from the operating system, or the application attempting to access the local storage device, that the action has failed.

◆ **Read Only:** Enables read access and disable write access. When users attempt to write to the device, they receive an error message from the operating system, or the application attempting to access the local storage device, that the action has failed.

◆ **Inherit:** Inherits this setting from other Storage Device Control policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Storage Device Control policies assigned to the user's groups, folders, or zone.

A.8.3 Enable Preferred Device List in the Policy

The *Removable Storage* access setting applies to all removable storage devices (RSDs). This includes FireWire devices, storage cards, USB devices, and any other devices reported as removable storage under *Disk drives* in Windows Device Manager.

The *Preferred Device* list applies only to USB devices. Select this option if you want to override the *Removable Storage* access setting for specific USB devices.

Default Device Access

Each device you add to the *Preferred Device* list must include an access assignment. The *Default Device Access* setting is used as the default access assignment for 1) any device you import that doesn't have an assignment and 2) any device you create whose access you set to *Default Access*. Select from the following options:

◆ **Enable:** Enables read and write access.

◆ **Disable:** Prevents read and write access. When users attempt to access files on the device, they receive an error message that the action has failed.

◆ **Read Only:** Enables read access and disable write access. When users attempt to write to the device, they receive an error message that the action has failed.

◆ **Inherit:** Inherits this setting from other Storage Device Control policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Storage Device Control policies assigned to the user's groups, folders, or zone.

Preferred Device List

The following table provides instructions for managing the *Preferred Device* list:

Task	Steps	Additional Details
Create a new device	1. Click *Add > Create New*. 2. Fill in the following fields: **Name:** Specify a name to identify the device in the ZENworks system. This name is required, but is not used to determine device matches, so it can be any name. **Serial Number:** Specify the device's serial number. This is an exact match field. If the serial number you enter is not identical to the serial number of the detected device, the detected device is not a match. The serial number and description are the two fields used to determine if a detected device matches this definition. You must fill in at least one of the fields. **Description:** Specify the device description. This is a partial match field, meaning that the description only needs to match any part of a device's description. For example, *Device1* not only matches *Device1* but also matches *Device10* and *USB Device100*. The more complete the description, the more specific the match. **Comment:** Specify any text you want to help identify the device in your system. This field is not used to determine device matches. **Access:** Select *Enable* to provide full read/write access. Select *Disable* to prevent all access. Select *Read Only* to provide read access but block write access. Select *Default Access* to use the *Default Device Access* setting. 3. Click *OK* to add the device to the list.	
Copy an existing device from another policy	1. Click *Add > Copy Existing*. 2. Select the Storage Device Control policies whose devices you want to copy. 3. Click *OK*.	All devices included in the other Storage Device Control policies are copied. If necessary, you can edit the copied devices after they are added to the list.

Task	Steps	Additional Details
Import a device from a policy export file	1. Click *Add > Import*. 2. Click 🔍 to display the Select File dialog box. 3. Click *Browse*, select the export file, then click *OK*. 4. Click *OK* to add the devices to the list.	All devices included in the export file are imported. If necessary, you can edit the imported devices after they are added to the list. For information about exporting devices, see Export a device.
Edit a device	1. Click the device name. 2. Modify the fields as desired. 3. Click *OK*.	
Export a device	1. Select the check box next to the device name. You can select multiple devices to export. 2. Click *Edit > Export*. 3. Save the file. The default name given to the file is `sharedComponents.xml`. You can change the name if desired. Do not change the `.xml` extension.	
Delete a device	1. Select the check box next to the device name, then click *Delete*. 2. Click *OK* to confirm deletion of the device.	

A.9 USB Connectivity Policy

The following instructions assume that you are on the *Configure USB Connectivity Settings* page in the Create New USB Connectivity Policy Wizard (see Chapter 9, "Creating Security Policies," on page 37) or that you are on the *Details* page for an existing USB Connectivity policy (see Chapter 13, "Editing a Policy's Details," on page 51).

The USB Connectivity policy lets you control whether or not a device supports USB devices. You can allow all USB devices, block all USB devices, or control access for groups or individual USB devices based on attributes such as Device Class, Manufacturer, Product, and Serial Number.

- Section A.9.1, "USB Devices," on page 132
- Section A.9.2, "Default Device Access," on page 133
- Section A.9.3, "Device Group Access Settings," on page 133
- Section A.9.4, "USB Device Access Settings," on page 134
- Section A.9.5, "Conflict Resolution," on page 137

A.9.1 USB Devices

Select whether or not USB connections are supported:

- **Enable:** Enables support for USB connections by keeping a device's USB bus active. You can then enable or disable access for groups of USB devices or individual devices.

- **Disable:** Disables support for USB connections by deactivating a device's USB bus. All USB devices (keyboards, mice, storage devices, and so forth) are disabled. If you select this option, the remaining options (*Default Device Access*, *Device Group Access Settings*, and *USB Device Access Settings*) do not apply and are disabled.
- **Inherit:** Inherits this setting from other USB Connectivity policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any USB Connectivity policies assigned to the user's groups, folders, or zone.

A.9.2 Default Device Access

Some USB devices might not match any of the device groups or individual devices you define in this policy. Select the default access (*Enable*, *Disable*, or *Inherit*) to assign to those USB devices.

A.9.3 Device Group Access Settings

Many USB devices fall into one of the four groups shown in the following table:

Device Group	Base Class Code	Examples
Human Interface Device (HID)	03h	Mice, keyboards, game controllers
Mass Storage Class	08h	Flash drives, external hard drives, personal digital assistants (PDAs), mobile phones, cameras, Windows portable devices (WPDs)
Printing Class	07h	Printers
Scanning/Imaging (PTP)	06h	Scanners, any device that uses the Picture Transfer Protocol

You specify access settings for each of the groups. When a device's base class matches a group, the device receives the group's access setting.

The three most common uses for the device group access settings are to:

- Disable access for an entire device group such as the Scanning/Imaging (PTP) group.
- Create *whitelists* for device groups. To create a whitelist, you disable access for a device group and then use the *USB Device Access Settings* list to define the enabled devices. For example, you might disable all Mass Storage Class devices and then enable specific removable storage devices.
- Create *blacklists* for device groups. To create a blacklist, you enable access for a device group and then use the *USB Device Access Settings* list to define the disabled devices. For example, you might enable all Printing Class devices and then disable specific printers.

Select one of the following access settings for each group:

- **Always Disable:** Always disable access. This setting takes precedence over all other access settings for the group's devices.

  For example, assume that you set the Scanner/Imaging (PTP) group access to *Always Disable*. You then define a scanner in the *USB Device Access Settings* list and give it *Always Enable* access. The *Always Disable* access setting overrides the *Always Enable* access setting and the scanner is still

blocked. Or, in another USB Connectivity policy you set the Scanner/Imaging (PTP) group access to *Always Enable* and assign the two policies to the same user. The *Always Disable* access setting overrides the *Always Enable* setting.

Because a USB device can receive multiple access settings (group setting for this policy, device setting for this policy, and group or device settings for other USB Connectivity policies) but only one access setting can be enforced, you should make sure you understand how access conflicts are resolved.

- **Always Enable:** Always enable access. This setting takes precedence over all access settings for group members except *Always Disable*.

  For example, if a member of the group is also defined in the *USB Device Access Settings* list and assigned *Disable* access, this group access setting overrides that setting and allows access. However, if the device is given *Always Disable* access, that setting takes precedence and the device is disabled.

- **Disable:** Disable access. This setting takes precedence over the *Enable* setting.

  Use this setting to create a *whitelist* for the device group. For example, to create a whitelist for removable storage devices, set the Mass Storage Class access to *Disable* so that all removable storage devices are blocked. Then, use the *USB Device Access Settings* list to define the allowed removable storage devices (the whitelist) and assign *Always Enable* access to each device.

- **Enable:** Enable access.

  Use this setting to create a *blacklist* for the device group. For example, to create a blacklist for printers, set the Printing Class access to *Enable* so that all printers are allowed. Then, use the *USB Device Access Settings* list to define the disabled printers (the blacklist) and assign *Always Disable* access to each device.

- **Default Device Access:** Give the device group the access specified by the *Default Device Access* setting.

- **Inherit:** Inherit this setting from other USB Connectivity policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any USB Connectivity policies assigned to the user's groups, folders, or zone.

A.9.4 USB Device Access Settings

The device groups use one attribute (Device Class) as the match criterion. If you have devices whose access you want to control based on matching different or additional attributes, you can use the *USB Device Access Settings* list.

For example, assume that the only mass storage device you want to allow is the Acme USB2 drive. In the Device Group Access Settings, you set Mass Storage Class to *Disable*. You then add the Acme USB2 to the *USB Device Access Settings* list and set the access to *Always Enable*.

It is possible that a detected device might match multiple device groups or devices. When this occurs, only one access level is assigned to the device. For information about how conflicts are resolved, see Conflict Resolution.

The following table provides instructions for managing the *USB Device Access Settings* list:

Task	Steps	Additional Details
Create a new device	1. Click *Add* > *Create New*. 2. Select the access you want assigned to the device: ◆ **Always Disable:** Always disable access. This setting takes precedence over all other access settings for the device. ◆ **Always Enable:** Always enable access. This setting takes precedence over all access settings for the device except *Always Disable*. ◆ **Disable:** Disable access. This setting takes precedence over the *Enable* setting. ◆ **Enable:** Enable access. ◆ **Default Device Access:** Give the device the access specified by the *Default Device Access* setting. ◆ **Inherit:** Inherit this setting from other USB Connectivity policies assigned higher in the policy hierarchy. 3. Fill in the fields you want to use as the device filter. The fields or attributes that you define create the filter used to determine device matches. All fields in the filter must match an attribute provided by the device in order to have a match. If the device does not provide an attribute that is required, or if the provided attribute is incorrect, the device does not match. Be aware of the following when defining fields: ◆ All fields from *USB Version* to *BCD Device* are always supplied by USB devices. The other fields might or might not be supplied, or they might differ from one machine to another. Whenever possible, you should use the *USB Version* to *BCD Device* fields for your match criteria. ◆ All fields are exact matches with the exception of Manufacturer, Product, and Friendly Name, which allow partial matches. ◆ Fields are case-insensitive. ◆ The *Name* and *Comment* fields are not used in the filter. 4. Click *OK* to add the device to the list.	A USB device can receive multiple access settings (group setting for this policy, device setting for this policy, and group or device settings for other USB Connectivity policies), but only one access setting can be enforced. You should make sure you understand how access conflicts are resolved. You can use the access options to create a whitelist or a blacklist. For example: ◆ To create a blacklist for removable storage devices, use the Device Group Access Settings to set the Mass Storage Class access to *Enable*. Then, add the disabled removable storage devices (the blacklist) and assign *Always Disable* access to each device. ◆ To create a whitelist for printers, set the Printing Class access to *Disable* so that all printers are disabled. Then, use the *Device Group Access Settings* list to define the allowed printers (the whitelist) and assign *Always Enable* access to each device.

Task	Steps	Additional Details
Copy an existing device from another policy	1. Click *Add* > *Copy Existing*. 2. Select the USB Connectivity policies whose devices you want to copy. 3. Click *OK*.	All devices included in the other USB Connectivity policies are copied. If necessary, you can edit the copied devices after they are added to the list.
Import a device from a policy export file	1. Click *Add* > *Import*. 2. Click 🔍 to display the Select File dialog box. 3. Click *Browse*, select the export file, then click *Open*. 4. Click *OK* to add the devices to the list.	All devices included in the export file are imported. If necessary, you can edit the imported devices after they are added to the list. For information about exporting devices, see Export a device.
Enable or disable a device	1. Locate the device in the list 2. In the Enabled column, select the check box to enable the device. or Deselect the check box to disable the device.	When you add a device, it is enabled by default. You can disable a device to save it in the policy but no longer have it applied.
Edit a device	1. Click the device name. 2. Modify the fields as desired. 3. Click *OK*.	
Rename an device	1. Select the check box next to the device name, then click *Edit* > *Rename*. 2. Modify the name as desired. 3. Click *OK*.	
Export a device	1. Select the check box next to the device name. You can select multiple devices to export. 2. Click *Edit* > *Export*. 3. Save the file. The default name given to the file is sharedComponents.xml. You can change the name if desired. Do not change the .xml extension.	
Delete a device	1. Select the check box next to the device name, then click *Delete*. 2. Click *OK* to confirm deletion of the device.	

A.9.5 Conflict Resolution

When a device is detected, its attributes (Device Class, Manufacturer, Product, and so forth) are compared to the attributes associated with the device groups in the *Device Groups Access Settings* list and the devices in the *USB Device Access Settings* list. In some cases, the device might match more than one group and device. For example, a removable storage device defined in the *USB Device Access Settings* list would also match the Mass Storage Class group.

In order to know which access setting to apply to a USB device, the Endpoint Security Agent uses the USB Connectivity policy to build an access filter to evaluate devices. If multiple USB Connectivity policies apply, the Endpoint Security Agent uses all of the policies to build the access filter.

The filter includes each access setting (Always Disable, Always Enable, and Allow) and the device groups and devices assigned to the setting. For example, assume the following group and device assignments for each access setting:

Access Setting	Group Assignments	Device Assignment
Always Disable		Mouse1
		Thumbdrive5, Thumbdrive2
Always Enable	Human Interface Device	Printer4, Printer3, Printer1
Disable	Printing Class	Scanner1
Block	Mass Storage Class	Printer2
	Scanning/Imaging (PTP	

A USB device is evaluated against the filter beginning with the highest-priority setting (*Always Disable*) and continuing to the lowest-priority setting (*Enable*). If the device matches one of the device groups or devices assigned to the access setting, the device receives that access setting and the evaluation ends.

Consider the following examples:

- Mouse1(a Human Interface Device) is detected. It is evaluated against the first setting (*Always Disable*). Because Mouse1 matches the Mouse1 device assignment for the *Always Disable* setting, Mouse1 is blocked and no further evaluation is required.

- Mouse4 (a Human Interface Device) is detected. It is evaluated against the *Always Disable* setting. Mouse4 does not match any *Always Disable* assignments (group or device), so it is evaluated against the *Always Enable* assignments. Because Mouse4 is a Human Interface Device and that device group is assigned the *Always Enable* setting, Mouse4 is allowed and no further evaluation is required.

- Thumbdrive1 and Thumbdrive5 (two Mass Storage Class devices) are detected. Thumbdrive5 is blocked because *Always Disable* (the device assignment) takes priority over Enable (the *Mass Storage Class* group assignment). Thumbdrive1 is allowed because it is included in the *Mass Storage Class* group assignment (*Enable*) and it does not match a device assignment.

- Printer2 and Printer4 (two Printing Class devices) are detected. Printer4 is allowed because *Always Enable* (the device assignment) takes priority over *Disable* (the *Printing Class* group assignment). Printer2 is blocked because *Disable* (the *Printing Class* group assignment) takes priority over *Enable* (the device assignment).

A.10   VPN Enforcement Policy

The following instructions assume that you are on the *Configure VPN Enforcement Settings* page in the Create New VPN Enforcement Policy Wizard (see Chapter 9, "Creating Security Policies," on page 37) or that you are on the *Details* page for an existing VPN Enforcement policy (see Chapter 13, "Editing a Policy's Details," on page 51).

The VPN Enforcement policy lets you configure VPN connection settings, select locations for which you want to enforce the use of the VPN connection, and select the location security settings you want applied during the VPN connection.

Typically, the VPN Enforcement policy is used to provide greater security at locations such as public wireless hotspots. For example, assume that you define a location called *Wireless Hotspot* to cover all public networks. You also define a location called *Wireless Hotspot VPN* that applies a Firewall policy that closes all ports, protocols, and addresses other than your VPN server's IP address. When the Endpoint Security Agent determines that it is in the Wireless Hotspot location, it switches to the Wireless Hotspot VPN location, applies the new location's security settings, then enforces a VPN connection.

To use the VPN Enforcement policy, you must have at least two defined locations (*Configuration* tab > *Locations* tab). One of them can be the predefined Unknown location.

- Section A.10.1, "Location Criteria," on page 138
- Section A.10.2, "Connect Settings," on page 138

A.10.1   Location Criteria

You use the Location Criteria settings to select the locations where you want to enforce a VPN connection and the location whose security settings you want to apply once the VPN connection is active.

- **Trigger Locations:** Specify the locations where you want to require the use of a VPN connection. To specify a location, click *Add*, select the location, then click *OK* to add it to the list.

- **Switch to Location:** Select the location whose security settings you want applied when the VPN connection is established. Typically, this should be a unique location that you created for use with VPN Enforcement policies. An example might be a location that has a Firewall policy that blocks all ports, protocols, and addresses except the one required for the VPN connection.

  Once the Endpoint Security Agent switches to this location, the device's user cannot manually change from the location, even if the location and the target location both allow manual user changes. The location remains in effect until a network environment change or a scripting policy forces a change in the location.

A.10.2   Connect Settings

You use the Connect Settings to define the VPN connection commands. You can also define a message for the Endpoint Security Agent to display to the user prior to the connection.

- "Use Connect Command" on page 139
- "Use Disconnect Command" on page 139
- "Use VPN Message" on page 139

Use Connect Command

This option lets you automatically launch the VPN client when the location switch occurs. If you don't want the VPN client automatically launched, you can use the *Use VPN Message* option instead.

Select the option, then fill in the following fields:

- **Link:** Specify the executable path for the VPN client.
- **Parameters:** Specify any parameters you want used when launching the client. Enter the parameters in the format required by the client.

Use Disconnect Command

This option lets you specify a command to execute if the VPN client becomes disconnected. For example, you might specify the command needed to reconnect.

Select the option, then fill in the following fields:

- **Link:** Specify the command to execute.
- **Parameters:** Specify any parameters associated with the command.

Use VPN Message

This option lets you display a message to the user. Additionally, you can include a hyperlink that enables the user to launch the VPN client.

For example, if you selected the *Use Connect Command* option, you might provide a message informing the user that his or her current location requires a VPN connection to maintain security. The Endpoint Security Agent displays the message before launching the VPN client.

Or, you can use this option without the *Use Connect Command* option. In this case, you would provide a message and a link to the VPN client. The user would then click the link to launch the client.

Select the option, then fill in the following fields:

- **Title of Message Window:** Specify the Message Window's title. For example, "VPN Connection Required".
- **Body:** Provide the text for the message body.
- **Message Hyperlink:** If you want to include hyperlink, select *Include message hyperlink*, then specify the display text for the hyperlink and the link command.

A.11 Wi-Fi Policy

The following instructions assume that you are on the *Configure Wi-Fi Settings* page in the Create New Wi-Fi Policy Wizard (see Chapter 9, "Creating Security Policies," on page 37) or that you are on the *Details* page for an existing Wi-Fi policy (see Chapter 13, "Editing a Policy's Details," on page 51).

The Wi-Fi policy lets you control wireless access

- Section A.11.1, "General Settings," on page 140
- Section A.11.2, "Access Points," on page 140
- Section A.11.3, "Minimum Security," on page 142
- Section A.11.4, "Minimum Security Message," on page 142

A.11.1 General Settings

The General Settings apply only to global policies. The settings are not displayed in a location-based policy.

- "Ad Hoc Connections" on page 140
- "Wi-Fi Connections" on page 140

Ad Hoc Connections

Ad hoc network connections provide peer-to-peer wireless access between devices. These connections are temporary but can be used for transferring files, playing multi-player computer games, and sharing Internet connection. Select one of the following options to control ad hoc connections:

- **Enable:** Allows ad hoc network connections.
- **Disable:** Prevents ad hoc network connections.
- **Inherit:** Inherits this setting from other Wi-Fi policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Wi-Fi policies assigned to the user's groups, folders, or zone.

Wi-Fi Connections

This setting lets you control Wi-Fi connectivity. Select one of the following options:

- **Enable:** Allows Wi-Fi connections.
- **Disable:** Prevents Wi-Fi connections. Connections are blocked but the wireless adapter remains active in case you want to use wireless access points to determine location. To completely disable Wi-Fi adapters, use the Communication Hardware policy.
- **Inherit:** Inherits this setting from other Wi-Fi policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Wi-Fi policies assigned to the user's groups, folders, or zone.

A.11.2 Access Points

You can use the *Access Points* list to control connections to wireless access points. The list works as follows:

- When you add an access point, you designate it as prohibited or approved. Prohibited access points are filtered out of a device's wireless network connection display. If a user manually connects to a prohibited access point, the connection is blocked.
- All access points are approved (default approval) until you add one approved access point to the list (explicit approval). At that point, the default approval is ignored and only explicitly approved access points are allowed.
- Prohibited access overrides approved access. For example, assume that you have multiple access points that share *Novell* as the SSID. You create an approved access point definition using Novell as the SSID, which results in all access points that share the Novell SSID being allowed. However, there is one Novell access point you want to prohibit, so you create a prohibited access point definition using the access point's MAC address. Based on its SSID and MAC address, the access point matches both definitions (approved and prohibited). Prohibited access overrides approved access, so connection to the access point is prohibited.

The following table provides instructions for managing access points:

Task	Steps	Additional Details
Add a new access point	1. Click *Add* > *Create New*. 2. Fill in the following fields to define the access point: **Name:** Specify a name to identify the access point in the ZENworks system. **SSID and MAC Address:** The *SSID* and the *MAC Address* are the two fields used to determine if a detected access point matches this definition. You must fill in at least one of the fields. Multiple access points can share the same SSID. If you fill in the *SSID* field, any access point that uses that SSID is matched. The SSID is case-sensitive. If you want to identify a specific access point, specify the MAC address. Each access point has a unique MAC address. **Enforcement:** Select whether the access point is prohibited or approved. 3. To define another access point, select *Define another access point*. 4. Click *OK* to add the access point to the list.	
Copy an access point from another policy	1. Click *Add* > *Copy Existing*. 2. Select the Wireless policies whose access points you want to copy. 3. Click *OK*.	All access points included in the selected Wireless policies are copied. If necessary, you can edit the copied access points after they are added to the list.
Import an access point from a policy export file	1. Click *Add* > *Import*. 2. Click 🔍 to display the Select File dialog box. 3. Click *Browse*, select the export file, then click *Open*. 4. Click *OK* to add the access points to the list.	All access points included in the export file are imported. If necessary, you can edit the imported access points after they are added to the list. For information about exporting access points, see Export an access point.
Edit an access point	1. Click the access point name. 2. Modify the fields as desired. 3. Click *OK*.	

Task	Steps	Additional Details
Export an access point	1. Select the check box next to the access point name. You can select multiple access points to export. 2. Click *Edit > Export*. 3. Save the file. The default name given to the file is `sharedComponents.xml`. You can change the name if desired. Do not change the `.xml` extension.	
Delete an access point	1. Select the check box next to the access point name, then click *Delete*. 2. Click *OK* to confirm deletion of the access point.	

A.11.3 Minimum Security

Select the minimum security protocol that an approved access point must provide before a connection is allowed. For example, if you select *WPA*, only approved access points that provide WPA or WPA2 encryption are allowed.

Select *No encryption required* to ignore minimum security. Select *Inherit* to inherit the minimum security from other Wi-Fi policies assigned higher in the policy hierarchy. For example, if you assign this policy to a user, the setting is inherited from any Wi-Fi policies assigned to the user's groups, folders, or zone.

Approved access points that fall below the minimum security level are not displayed in the device's wireless network connections list when detected. If a user tries to manually define a connection to the access point, the connection is blocked.

A.11.4 Minimum Security Message

This option is available only if you selected *WEP*, *WPA*, or *WPA2* as the minimum security requirement.

You can display a message when a wireless connection is blocked because the access point does not meet the minimum security requirement. Select *Display message when minimum security not met*, then fill in the following fields:

- **Title of Message Window:** Specify the message window's title.
- **Body:** Provide the text for the message body.
- **Message Hyperlink:** If you want to include a hyperlink, select *Include message hyperlink*, then specify the display text for the hyperlink and the link command.

B Security Policy Summary

The following chart provides a summary of location support (global or location-based), assignment support (device, user, or zone), and multiple-policy support (plural or singular).

	Global	Location-Based	Device Assignment	User Assignment	Zone Assignment	Plural	Singular
Application Control	✓	✓	✓	✓	✓	✓	
Communication Hardware	✓	✓	✓	✓	✓	✓	
Data Encryption	✓		✓		✓		✓
Firewall	✓	✓	✓	✓	✓	✓	
Location Assignment	✓		✓	✓	✓	✓	
Security Setting	✓		✓	✓	✓	✓	
Storage Device Control	✓	✓	✓	✓	✓	✓	
USB Connectivity	✓	✓	✓	✓	✓	✓	
VPN Enforcement	✓		✓	✓	✓		✓
Wi-Fi	✓	✓	✓	✓	✓	✓	

Global: Can be created as a global policy. A global policy is available regardless of the device's location.

Location-Based: Can be created as a location-based policy. A location-based policy is available only when the device's location matches a location defined in the policy.

Device Assignment: Can be assigned to a device, device folder, or device group.

User Assignment: Can be assigned to a user, user folder, or user group.

Zone Assignment: Can be assigned as a default policy at the Management Zone.

Plural: Supports merging of multiple policies (of the same type) into one effective policy to be enforced on a device. The effective policy is a determined by established ordering and merging rules. For details, see Chapter 5, "Effective Policies," on page 19.

Singular: Supports enforcement of only one policy (of a single type) on a device. If multiple policies are assigned, the effective policy is determined by established ordering rules. For details, see Chapter 5, "Effective Policies," on page 19.

C Naming Conventions in ZENworks Control Center

When you name an object in ZENworks Control Center (folders, bundles, policies, groups, registration keys, and so forth), ensure that the name adheres to the following conventions:

- The name must be unique in the folder.
- Depending on the database being used for the ZENworks database, uppercase and lowercase letters might not create uniqueness for the same name. The embedded database included with ZENworks 11 is case insensitive, so Folder 1 and FOLDER 1 are the same name and cannot be used in the same folder. If you use an external database that is case-sensitive, Folder 1 and FOLDER 1 are unique.
- If you use spaces, you must enclose the name in quotes when you enter it on the command line. For example, you must enclose reg key 1 in quotes ("reg key 1") when you enter it in the zman utility.
- The following characters are invalid and cannot be used: / \ * ? : " ' < > | ` % ~

D Documentation Updates

This section contains information on documentation content changes that were made in this Endpoint Security Policies Reference since its initial publication.

The documentation was updated on the following dates:

- Section D.1, "March 20, 2012: Support Pack 2," on page 147

D.1 March 20, 2012: Support Pack 2

Location	Update
All sections	Updated screen shots to new version
Script Development and Testing	Moved the scripting appendixes to a new guide for easier accessibility. See the *ZENworks 11 SP2 Endpoint Security Scripting Reference*.
Chapter 2, "Types of Security Policies," on page 13	Added information to Security Settings policy entry to explain that the security settings are now part of the ZENworks Agent configuration settings (*Configuration > Management Zone Settings > Device Management > ZENworks Agent*). The policy still applies to devices running earlier versions of the ZENworks Adaptive Agent.
Chapter 9, "Creating Security Policies," on page 37	Changed steps to reflect changes to Create New Policy Wizard. You now select the platform as the first step of the wizard.